Vorentwurf zu einem Bundesgesetz über die elektronische Signatur (BGES)

Zusammenstellung der Vernehmlassungen

****

Avant-projet concernant une loi fédérale sur la signature électronique (LFSél)

Classement des réponses suite à la procédure de consultation

****

Avamprogetto concernente una legge federale sulla firma elettronica (LFiE)

Risultati della procedura di consultazione

September / septembre / settembre 2001

Inhaltsverzeichnis / Table des matières / Indice

1. Allgemeines / Généralités /Generalità

Das Vernehmlassungsverfahren dauerte vom 17. Januar bis 31. März 2001. Zur Vernehmlassung eingeladen wurden das Schweizerische Bundesgericht in Lausanne und das Eidgenössische Versicherungsgericht in Luzern, alle Kantone, die in der Bundesversammlung vertretenen Parteien und 45 Organisationen und Privatpersonen.

Die „economiesuisse“ und der „Schweizerische Gewerbeverband“ haben eine gemeinsame Stellungnahme eingereicht. Der „Verband Inside Telecom“ schliesst sich der Stellungnahme der „economiesuisse“ an. „Protelecom“ schliesst sich der Vernehmlassungsantwort der „Swiss Information and Communications Technology Association“ an.

****

La procédure de consultation a duré du 17 janvier au 31 mars 2001. Ont été invités à y participer le Tribunal fédéral suisse à Lausanne, le Tribunal fédéral des assurances à Lucerne, tous les cantons, les partis représentés à l'Assemblée fédérale ainsi que 45 organisations et personnes privées.

L'„Union suisse des arts et métiers“ et l'„économiesuisse“ ont fait une position commune. L'association „Inside Telecom“ se rallie à la prise de position de l'„economiesuisse“. „Protelecom“ se rallie à la prise de position de „Swiss Information and Communications Technology Association“.

****

La procedura di consultazione è durata dal 17 gennaio al 31 marzo 2001. Sono stati invitati a partecipare alla stessa il Tribunale federale svizzero di Losanna, il Tribunale federale delle Assicurazioni di Lucerna, tutti i cantoni, i partiti rappresentati nell'Assemblea federale e 45 organizzazioni e privati.

L'„Unione svizzera delle arti e mestieri“ e „economiesuisse“ hanno inoltrato una presa di posizione comune. „Inside Telecom“ si associa all'avvsio di „economiesuisse“, „Protelecom“ a quello della „Swiss Information and Communications Technology Association“.

****

2. Verzeichnis der Eingaben
Liste des organisations ayant répondu
Elenco dei partecipanti

(in der Zusammenstellung verwendete Abkürzungen sind vorangestellt)
(dans le classement, les abréviations précèdent les avis)
(nel riassunto, le abbreviazioni precedono i pareri)

Gerichte / Tribunaux / Tribunali

BGr Bundesgericht / Tribunal fédéral / Tribunale federale

Kantone / Cantons / Cantoni

AG Aargau / Argovie / Argovia
AI Appenzell Innerrhoden / Appenzell Rh.-Int. / Appenzello Interno
AR Appenzell Ausserrhoden / Appenzel Rh.-Ext. / Appenzello Esterno
BE Bern / Berne / Berna
BL Basel-Land / Bâle-Campagne / Basilea-Campagna
BS Basel-Stadt / Bâle-Ville / Basilea-Città
FR Freiburg / Fribourg / Friburgo
GE Genf / Genève / Ginevra
GL Glarus / Glaris / Glarona
GR Graubünden / Grisons / Grigioni / Grischun
JU Jura / Jura / Giura
LU Luzern / Lucerne / Lucerna
NE Neuenburg / Neuchâtel
NW Nidwalden / Nidwald / Nidvaldo
OW Obwalden / Obwald / Obvaldo
SG St. Gallen / St-Gall / San Gallo
SH Schaffhausen / Schaffhouse / Sciaffusa
SZ Schwyz / Schwyz / Svitto
SO Solothurn / Soleure / Soletta
TG Thurgau / Thurgovie / Turgovia
TI Tessin / Tessin / Ticino
UR Uri
VD Waadt / Vaud
VS Wallis / Valais / Vallese
ZG Zug / Zoug / Zugo
ZH Zürich / Zurich / Zurigo

Parteien / Partis politiques / Partiti politici

CVP	Christlichdemokratische Volkspartei Parti Démocrate-Chrétien Partito Popolare Democratico
FDP	Freisinnig-Demokratische Partei der Schweiz Parti radical-démocratique suisse (PRD) Partito liberale-radicale svizzero (PLR)
Jungfreisinnige	Jungfreisinnige Schweiz Jeunes Radicaux Suisses Giovani Liberali Radicali Svizzeri
PLS	Parti libéral suisse Liberale Partei der Schweiz
SVP	Schweizerische Volkspartei Union Démocratique du Centre (UDC) Unione Democratica di Centro (UDC)

Interessierte Organisationen / Organisations intéressées / Organizzazioni interessate

Briner	Pestalozzi / Gmür / Patry, Rechtsanwälte, Zürich
camera commercio	Camera commercio industria artigianato cantone Ticino
Clusis	Association suisse de la sécurité des systèmes d'information Schweizerischer Verband der Sicherheit von Informationssystemen Associazione svizzera della sicurezza dei sistemi d'informazione
CP	Centre Patronal
DigiSigna	Elektronischer Registrier- und Zertifizierdienst der Schweizer Handelskammern Service d'enregistrement et de certification électronique des Chambres de commerce suisses Servizio di registrazione e certificazione elettronica delle Camere di commercio svizzere
Distefora	DISTEFORA Mobile (Switzerland) AG
DSB	Die Schweizerischen Datenschutzbeauftragten Les Commissaires suisses à la protection des données
economiesuisse	Verband der Schweizer Unternehmen Fédération des entreprises suisses Federazione delle imprese svizzere
EKK	Eidgenössische Kommission für Konsumentenfragen Commission fédérale de la consommation Commissione federale del consumo
FGSec	Schweizer Informatiker Gesellschaft, Fachgruppe Security (Arbeitsgruppe PKI)
FHZ	Hochschule für Wirtschaft Luzern / Institut für Wirtschaftsinformatik
FRC	Fédération romande des consommateurs
FRI	Fédération romande immobilière
FSP	Fédération Romande des Syndicats Patronaux

ISACA	Information Systems Audit and Control Association
Jeune Barreau vaudois	Jeune Barreau vaudois
kf	Konsumentenforum deutsche Schweiz
KVN	Konsumenten-Vereinigung-Nordwestschweiz
KPMG	KPMG
Kunststoff-verband	Kunststoffverband Schweiz
Landestop	Bundesamt für Landestopographie
Muster/Sury	Daniel Muster, Zürich / Ursula Sury, Luzern
protelecom	Schweizerische Vereinigung der Telekommunikation
Rosenthal	Lic.iur. David Rosenthal, Basel
SAV	Schweizerischer Anwaltsverband Fédération Suisse des Avocats (FSA) Federazione Sivzzera degli Avvocati (FSA)
SBB	Schweizerische Bundesbahnen Chemins de fer fédéraux (CFF) Ferrovie federali svizzere (FFS)
Schlauri/Kohlas	Lic. iur. Simon Schlauri, Zürich / Reto Kohlas
SBV	Schweizerische Bankiervereinigung Association suisse des banquiers (ASB) Associazione svizzera dei banchieri (ASB)
SGB	Schweiz. Gewerkschaftsbund Union syndicale suisse (USS) Unione sindacale svizzera (USS)
SGV	Schweizerischer Gewerbeverband Union suisse des arts et métiers Unione svizzera delle arti e mestieri
SfK	Stiftung für Konsumentenschutz
SICTA	Swiss Information and Communications Technology Association
SIK	Schweizerische Informatikkonferenz Conférence Suisse sur l'Informatique Conferenza svizzera sull'informatica
SWICO	Schweizerischer Wirtschaftsverband der Informations-, Kommunikations- und Organisationstechnik
SwissITC	Schweizerischer Verband der Informations- und Kommunikationstechnologie
SVV	Schweizerischer Versicherungsverband Association Suisse d'Assurances (ASA) Associazione Svizzera d'Assicurazioni (ASA)
SUISA	Schweizerische Gesellschaft für die Rechte der Urheber musikalischer Werke Société suisse pour les droits des auteurs d'œuvres musicales Società svizzera per i diritti degli autori di opere musicali
swisscom	swisscom AG
Swisskey	Swisskey AG, Zürich

Treuhand-kammer	Schweizerische Kammer der Wirtschaftsprüfer, Steuerexperten und Treuhandexperten
TSM	Treuhandstelle Milch GmbH
Vischer	Prof. Dr. iur. Dr. iur. h.c. Frank Vischer, Basel
VIT	Verband Inside Telecom (VIT) der Telekommunikationsnetz- und Mehrwertdiensteanbieter
VSG	Verband Schweizerischer Grundbuchverwalter Société suisse des conservateurs du registre foncier Società svizzera degli ufficiali del registro fondiario
VSW	Verband Schweizerischer Werbegesellschaften Association des Sociétées Suisses de Publicité (ASSP) Associazione delle Società Svizzere di Pubblicità (ASSP)

3. Zusammenstellung der Vernehmlassungen
Classement des réponses suite à la procédure de consultation
Risultati della procedura di consultazione

31 Im Allgemeinen / En général / In generale

311 Positive Gesamtbeurteilung des Vorentwurfs
Appréciation générale positive de l'avant-projet
Giudizio generale positivo sull'avamprogetto

Kantone / Cantons / Cantoni

AG Dem unterbreiteten Entwurf für ein Bundesgesetz über die elektronische Signatur (BGES) können wir insgesamt zustimmen. Allerdings muss betont werden, dass der Entwurf nicht die elektronische Signatur an sich, sondern Anerkennungsvoraussetzungen sowie Rechte und Pflichten der Anbieter von Zertifizierungsdiensten regelt. Von zentraler Bedeutung ist der neue Artikel 15a OR, der die elektronische Signatur der eigenhändigen Unterschrift dann gleichsetzt, wenn erstere auf dem Zertifikat eines anerkannten Anbieters von Zertifizierungsdiensten im Sinne des BGES beruht.
Eine solche Gleichsetzung ist im schweizerischen Zivilrecht längst fällig, da bereits heute viele Verträge über wesentliche geldwerte Leistungen elektronisch zustande kommen. Dies nicht nur im eigentlichen E-Commerce, wo sich der Anbieter über die Informations-Technologie ans Publikum wendet, sondern auch im bilateralen Verkehr unter Geschäftsleuten. Um Missbrauchstatbestände möglichst auszuschliessen und Sicherheit für die Parteien zu schaffen, muss von den Parteien gewollte oder vorgeschriebene Schriftlichkeit auch in einer elektronischen Variante von Gesetzes wegen möglich sein. Die Formulierung des Art. 15a OR ist einfach, klar und verständlich. Mit dem Verweis auf die Anerkennung nach BGES ist auch klar, dass sich die Vertragswilligen nur auf elektronische Signaturen mit qualifiziertem Zertifikat verlassen können.

AI Die Zielsetzungen des Bundesgesetzes über die elektronische Signatur, ein breites Angebot an sicheren Diensten der elektronischen Zertifizierung zu fördern und die Gleichstellung (in gewissen Bereichen) der elektronischen Signatur mit der eigenhändigen Unterschrift sicherzustellen, werden ausdrücklich begrüsst. Die Anpassungskompetenz zu Handen des Bundesrates wird als sinnvoll erachtet, kann doch die technische Entwicklung - gerade auch in diesem Bereich - nicht vorausgesehen werden.

AR Die Tatsache, dass im privaten Rechtsverkehr mit elektronischen Signaturen gearbeitet werden kann, lässt ohne Zweifel den Druck auf die öffentliche Verwaltung, dieses Instrument ebenfalls einzusetzen, steigen. Es ist in der Tat schwer einsehbar, weshalb ein elektronisch signierter Vertrag rechtsgültig sein soll, eine elektronisch signierte Steuererklärung indessen nicht. Dabei ist darauf hinzuweisen, dass die Umstellung auf eine elektronische Kommunikation von Bürgern und Behörden die personellen und finanziellen Ressourcen des Kantons erheblich beanspruchen wird. Zudem sind allfällige Schwierigkeiten aufgrund der verschiedenen Standards bei den betroffenen Behörden zu beachten.
Trotz der dargestellten Folgen bildet die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift eine Basisvoraussetzung für die Möglichkeit, beispielsweise die Steuererklärung elektronisch einreichen zu

können. Die Bestrebungen dazu sind in vollem Gang. Eine gesetzliche Regelung der elektronischen Signatur ist daher unumgänglich.

BE Das Bundesgesetz über die elektronische Signatur (BGES) setzt die mit dem neuen Art. 15a OR vorgesehene rechtliche Gleichstellung der elektronischen Signatur mit der persönlichen Unterschrift um und ist für die künftige Entwicklung des Geschäfts- und Dienstleistungsverkehrs sowie für den Geschäftsstandort Schweiz von hoher Bedeutung. Die angestrebte Übereinstimmung mit dem europäischen Recht scheint uns im Hinblick auf die zunehmende Globalisierung der Märkte richtig. Bedingt durch die rasche Entwicklung der Technik erachten wir es auch als angebracht, alle technischen Aspekte aus dem Gesetz auszuklammern und in technischen Richtlinien festzuhalten. Immerhin kommen wir nicht umhin, einem gewissen Unbehagen Ausdruck zu verleihen, was die technische Sicherheit der elektronischen Signatur anbelangt. Solange die Umgebung, in welche die elektronische Signatur implementiert wird, nicht sicherer gemacht wird, zum Beispiel durch zusätzlichen Kostenaufwand für die Umgebung der Betriebssysteme, indem neue Hardwarekomponenten direkt miteinander verbunden werden, wird es schwer sein, das für den Erfolg der elektronischen Signatur notwendige Vertrauen zu schaffen. Ferner sehen wir die Gefahr, dass beim Einsatz im privaten Bereich unberechtigte Zugriffe durch Kinder stattfinden können und diese mit Hilfe der elektronischen Signatur Verträge im Namen der Eltern abschliessen. Wir stellen in den Schulen immer wieder fest, dass die Kinder in der Anwendung der ICT den Eltern weit voraus sind.

BL Wir begrüssen die Absicht des Bundes, eine gesetzliche Grundlage zur Anerkennung der elektronischen Signatur und deren Gleichstellung mit der eigenhändigen Unterschrift zu schaffen. Der Vernehmlassungsentwurf bildet eine notwendige und taugliche Rechtsgrundlage für die sichere Weiterentwicklung der elektronischen Kommunikation. Dies führt zu einem Standortvorteil der Schweiz gegenüber anderen Ländern, die diesen Schritt noch nicht vollzogen haben.

Der Gesetzesentwurf gibt einen Hinweis darauf, dass die für elektronische Signaturen generell vorgesehene Technologie hohen Ansprüchen genügen könnte. Gemäss Art. 1 bezweckt das Gesetz denn auch die Förderung eines breiten Angebots an sicheren Diensten der elektronischen Zertifizierung. Ausgehend von diesem Zweckgedanken ist nicht nur die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift von Relevanz, sondern auch (oder gerade) die hierbei zugrundeliegende Technologie und insbesondere deren Förderung. Der Einsatz und die Verbreitung der Kryptographie sind wichtige Postulate im Interesse des Datenschutzes und der Datensicherheit, denn dank kryptographischer Verfahren kann für die elektronische Datenkommunikation nicht nur Verbindlichkeit, sondern auch Vertraulichkeit, Integrität und Authentizität gewährleistet werden.

BS Der Regierungsrat des Kantons Basel-Stadt begrüsst die Tatsache, dass sich der Bund mit der Frage der elektronischen Signatur, des E-Government und der elektronischen Dokumente auseinandergesetzt hat. Die elektronische Kommunikation wird weiter an Bedeutung zunehmen, so dass die Ausarbeitung entsprechender Normen rechtzeitig an die Hand genommen werden muss.

Die rasante technische Entwicklung insbesondere im Bereich des Internets hat zu Anwendungen geführt, deren Gebrauch für die Anwenderinnen und Anwender nicht nur mit technischen, sondern insbesondere auch mit erheblichen rechtlichen Problemen verbunden sind. Es werden wichtige, eventuell sogar

vertrauliche Daten via E-Mail ausgetauscht. Ebenso werden Verträge via E-Mail geschlossen. Es werden über Internet Aktien gekauft und verkauft, das Post- oder ein Bankkonto geführt und es werden Waren - womöglich noch in den verschiedensten Ländern - eingekauft. All diese Transaktionen sind aus rechtlicher Sicht eigentlich nur dann wirklich möglich, wenn die in den beschriebenen Formen miteinander kommunizierenden Personen, welche im Internet zunächst völlig anonym auftreten, klar identifiziert werden können. Elektronische Zertifikate oder digitale Unterschriften haben deshalb für diese, heute wohl erst am Anfang der Entwicklung stehende Form der Kommunikation eine essentielle Bedeutung. Aus diesem Grunde ist eine Regelung der Anwendung digitaler Signaturen oder elektronischer Zertifikate und insbesondere auch die Regelung des Verhältnisses zwischen eigenhändiger Unterschrift und digitaler Signatur unabdingbar und dringend erforderlich.

Im Wissen, dass andere Länder bereits heute entsprechende gesetzliche Regelungen getroffen haben und anwenden (Deutschland, Österreich, Italien, Frankreich usw.), ist es für die Schweiz dringend erforderlich, eine entsprechende gesetzliche Regelung einzuführen, um einerseits die Anwendung der digitalen Signatur rechtlich abzustützen und andererseits durch entsprechende rechtliche Grundlagen die Basis dafür zu schaffen, die Möglichkeiten der digitalen Signatur oder elektronischer Zertifikate ausschöpfen zu können. Es ist deshalb sehr zu begrüssen, dass der Bundesrat sein im Zusammenhang mit dem Erlass der Zertifizierungsdiensteverordnung abgegebenes Versprechen, möglichst rasch eine Vorlage vorzubereiten, welche die Anerkennung der elektronischen (digitalen) Signatur insbesondere im Privatrechtsverkehr regelt, innerhalb nur eines Jahres erfüllt hat.

Der Gesetzesentwurf geht von der Prämisse aus, dass die digitale Signatur - als einer der derzeit bedeutungsvollsten Anwendungsfälle elektronischer Signaturen - der eigenhändigen Unterschrift gleichgestellt werden soll. Aufgrund der rasanten Entwicklung im Bereich des elektronischen Handels (E-Commerce) ist dieser Prämisse zuzustimmen. Einen den Konsumentenschutz betreffenden Vorbehalt bringen wir allerdings (vgl. unter Ziff. 322.31) an. Die rasante Entwicklung in diesem Bereich zeigt auch, dass rasches Handeln dringend geboten ist, wenn die Schweiz international nicht in Rückstand geraten will.

FR Nous n'avons pas de remarques particulières à formuler sur ce projet qui, au demeurant, reprend en grande partie les dispositions de l'Ordonnance sur les services de certification électronique.

La loi en son ensemble n'entrave pas le développement technologique dans ce domaine, ce qui est réjouissant. L'utilisation large de la signature électronique nécessite toutefois que les autorités étatiques, en collaboration avec des instances internationales, promeuvent davantage les technologies adéquates pour les utilisateurs et participent à la certification d'installations informatiques. Les projets en cours dans ces domaines, par exemple „le guichet virtuel“, doivent être renforcés. La protection des données nécessite en effet que l'Etat s'investisse davantage, surtout si l'on considère qu'en assimilant la signature électronique à la signature manuscrite lors de la conclusion de contrats, la finalité en soi de la signature électronique est atteinte. Pourtant, la signature électronique sera le plus souvent utilisée pour s'assurer de la confidentialité d'envois électroniques, voire à titre de reconnaissance des utilisateurs. Ces derniers points constitueront en effet la principale raison d'être de la signature électronique.

En conclusion, le projet de loi permet aux cantons d'insister sur le fait que les installations nécessaires à la promotion de la signature électronique doivent être davantage développées.

GL Die Schaffung einer gesetzlichen Grundlage für den elektronischen Verkehr mit verschiedenen öffentlichen Registern wird sehr begrüsst. Der Gesetzesentwurf ist ein taugliches und notwendiges Instrument, um die digitale Signatur auch in jenen (wenigen) Fällen anzuerkennen, in denen die Gesetzgebung bisher für einen gültigen Vertragsabschluss eine handschriftliche Unterzeichnung verlangte. Hinsichtlich der Chancen einer weiten Verbreitung von digitalen Signaturen auf der Grundlage des vorliegenden Gesetzesentwurfs sind jedoch Zweifel anzubringen.

Im Licht der folgenden Erwägungen wird der Gesetzesentwurf als grundsätzliche Anerkennung der neuen Technologie zwar begrüsst. Bei der Verwendung der digitalen Signatur stellt deren Gleichstellung mit der handschriftlichen Unterschrift aber lediglich die oberste und eher wenig verwendete Stufe dar. Viel häufiger und von entsprechend grösserer Bedeutung für den Geschäftsverkehr ist jedoch die Verwendung der digitalen Signatur etwa für die Identifikation, sicheres E-Mailen oder den Abschluss formfreier Verträge. Auch hier besteht ein grosses Bedürfnis nach Wahrung der Integrität und Vertraulichkeit sowie Gewährleistung der Authentizität. Es ist daher sehr erwünscht, dass der Bund benutzerfreundliche Technologien fördert und insbesondere auch einzelne technische Komponenten zertifizieren hilft (vgl. Tendenzen in diese Richtung beim Projekt „guichet virtuel"). Gerade im Hinblick auf die Einführung von Electronic Government ist die Förderung sicherer IT-Komponenten ein vordringliches Anliegen der Kantone.

Aus unserer Sicht ist die noch fehlende Anerkennung elektronischer Signaturen ein klares Handicap auch im E-Government Bereich. Aus technischer Sicht bestehen heute die Hilfsmittel, um im Rahmen der elektronischen Kommunikation Informationen auszutauschen, die einen rechtsverbindlichen Charakter haben (elektronische Steuererklärung, Bestellung eines Fahrzeugausweises, Antrag auf ein Jagdpatent usw.). Die produktive Einführung solcher E-Government Lösungen ist im Wesentlichen nur deshalb noch nicht möglich, weil die rechtsverbindliche Anerkennung der elektronischen Signatur und die Anerkennung der Anbieterinnen von Zertifizierungsdiensten fehlt. Hier sind aus der Sicht des Regierungsrates entsprechende Schritte dringend geboten.

Im weiteren gilt auch hier, dass durch die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift ein weiterer Kommunikationsweg geöffnet, aber kein bestehender ersetzt wird. Es werden also in Zukunft neue Investitionen nötig sein, um im Bereich des E-Governments diese Möglichkeiten auch anbieten zu können. Dabei denken wir nicht nur beispielsweise an Hardware für die Erkennung und Validierung der elektronischen Signatur, sondern auch an Investitionen im Bereich der Datenspeicherung, Datenverfügbarkeit und Datenarchivierung.

Die gesetzliche Regelung steht dem technologischen Fortschritt aber insgesamt - was als durchaus positiv zu vermerken ist - nicht im Weg. Zur generellen Verbreitung der digitalen Signatur ist jedoch vorab erforderlich, dass der Bund - vermutlich in Zusammenarbeit mit internationalen Gremien - benutzerfreundliche Technologien fördert und technische Komponenten zertifizieren hilft. Bereits eingeleitete Aktivitäten in diese Richtung - etwa anlässlich des Projekts „guichet virtuel" - sind zu verstärken. Gerade aus der Sicht des Datenschutzes muss diese Forderung mit Nachdruck erhoben werden.

GE Notre Conseil se félicite de ce projet, qui vient à son heure compte tenu du développement des moyens de communication électroniques. Il est en effet du devoir de l'Etat de veiller à ce que les instruments légaux accompagnent - et non entravent - les développements spectaculaires que l'on peut pressentir en lien avec le commerce électronique. Cela participe à l'adaptation permanente des conditions cadres favorables à l'activité économique et à la prospérité des entreprises dans notre pays. En ce sens, la démarche du Conseil fédéral ne peut qu'être saluée et encouragée dans son principe, ce d'autant que la reconnaissance de la signature électronique constitue également un élément essentiel du développement, indispensable, de la cyberadministration.
Le canton de Genève, à l'instar de la réflexion conduite au niveau fédéral par la Confédération avec la création de son guichet virtuel, développe un concept de e-government intégrant notamment transaction ou téléprocédure, qui permet l'application de procédures à distance par Internet (par exemple : un changement d'adresse, une demande d'autorisation, un extrait officiel, etc.). Les questions à régler sont donc bel et bien celles de l'identification, de la sécurité de la transaction et de l'authentification de la prestation (le document doit être officiel et reconnu comme tel). Ces questions réglées permettront de garantir la protection de la sphère privée.
La mise en place de la signature électronique implique un cadre juridique adéquat et une technologie fiable (sécurité de la transaction). Cette condition préalable est nécessaire à la transaction. La reconnaissance juridique du document officiel en ligne constitue dès lors une nécessité.
Compte tenu d'une technologie qui évolue sans cesse, le champ d'application de la future loi doit permettre, dans un cadre suffisamment souple, la transformation des processus administratifs analogiques sous la forme digitale dans le cadre d'architectures technologiques utilisant une infrastructure à Clef Publique. Plusieurs modèles technologiques sont aujourd'hui opérationnels, par exemple la clef électronique ou la carte à puce en matière d'authentification de signature numérique et de certification électronique. Le fait que le législateur ait prévu que des administrations puissent être reconnues comme „fournisseur de service de certification“ est une excellente chose. Ainsi, ces administrations seront-elles libres de fournir leurs propres certificats ou de reconnaître ceux mis en place sur le marché : la mise en œuvre de la cyber administration en sera accélérée. Il est envisageable, par exemple, qu'un bureau de l'administration (ou d'une commune) délivre des certificats à ceux qui en font la demande, respectivement enregistre les certificats présentés.
En revanche, contrairement à ce que laisse entendre le rapport explicatif, le projet qui nous est soumis ne nous paraît pas respecter le principe de la neutralité technologique et, telle qu'elle est envisagée, la réglementation des rapports de droit privé créés par voie électronique appelle de sérieuses réserves.

GR Mit dem vorgeschlagenen Erlass wird ein klares Zeichen zugunsten der Entwicklung der Informationsgesellschaft in der Schweiz gesetzt. Es ist wichtig, dass die Schweiz im internationalen Vergleich den Anschluss keinesfalls verpasst. Die Vorlage hat, wenn sie auch nur wenige diesbezügliche spezifische Regelungen beinhaltet, auch eine Bedeutung für die weitere Förderung des elektronischen Behördenverkehrs (E-Government). Dabei kann es notwendig sein, die Fragen des elektronischen Verkehrs mit den Behörden zusätzlich einzelfallweise in weiteren Erlassen zu regeln.
Die Regierung begrüsst aus diesen Überlegungen grundsätzlich den vorliegenden Entwurf für ein Bundesgesetz über die elektronische Signatur und die be-

förderliche Behandlung. Bereits heute ist erkennbar, dass bei der Detailregelung und beim Vollzug, namentlich in den Kantonen, noch verschiedene rechtliche sowie technische und andere praktische Fragen zu lösen sein werden. Nicht transparent sind zur Zeit auch die indirekten Kostenfolgen, welche sich für die Kantone ergeben werden. Die Regierung erachtet es deshalb als unerlässlich, dass sich die Kantone zu den vom Bundesrat noch zu erlassenden Ausführungsvorschriften äussern können.

JU D'une manière générale, le Gouvernement de la République et Canton du Jura approuve l'objet et le but du projet de loi mis en consultation. En effet, en contribuant à combler un besoin de sécurité juridique s'agissant des transactions ou autres échanges d'information passés en la forme électronique, le projet de loi permet de répondre à des attentes légitimes. D'autre part, en prévoyant l'équivalence de la signature électronique à la signature manuscrite en droit des contrats, le projet permet une adaptation bienvenue de la législation face aux constants progrès technologiques.

LU Der Entwurf bildet unseres Erachtens eine taugliche Grundlage für den Einsatz der digitalen Signatur im Geschäftsverkehr. Um die erforderliche Sicherheit der digitalen Signatur zu garantieren, sind die Voraussetzungen zu Recht streng ausgestaltet, welche die Anbieterinnen von Zertifizierungsdiensten erfüllen müssen (Art. 4).

NE La loi qui est proposée s'écarte peu de l'ordonnance sur les services de certification électronique, à telle enseigne qu'on pourrait se demander s'il était véritablement nécessaire de procéder en deux étapes du moment où la durée de vie de l'ordonnance n'aura pas permis de tirer des enseignements de la pratique utiles à l'élaboration de la loi.

En tout état de cause, la signature électronique répond à un besoin de l'économie. Le degré de sécurité, qui selon le rapport, dépasse celui des déclarations écrites traditionnelles doit amener à revoir le Code des obligations qui ne prévoit que la signature manuscrite. Elle est réclamée par le développement naturel du commerce électronique et nous avons le plaisir de pouvoir vous dire que le présent projet qui tend à l'introduction de l'utilisation de cette signature est très bien accueilli par les différents acteurs du domaine que nous avons à notre tour consultés. Le seul regret exprimé à cette occasion se rapporte au fait que cette loi n'envisage pas de régler la question des relations entre les administrés et les autorités (cyberadministration) qui devra donc faire l'objet d'autres réformes.

NW Der Entwurf stellt ein taugliches und notwendiges Instrument dar, um die digitale Signatur auch in den seltenen Fällen zum Einsatz gelangen zu lassen, wo die Gesetzgebung bisher zu einem gültigen Vertragsschluss eine handschriftliche Unterzeichnung verlangte. Das Gesetz gibt damit einen Hinweis, dass die für digitale Signaturen generell vorgesehene Technologie hohen Ansprüchen genügen könnte. Denn nach Art. 1 des Bundesgesetzes über die elektronische Signatur (BGES) bezweckt es gleichfalls die Förderung eines breiten Angebotes an sicheren Diensten der elektronischen Zertifizierung. Ausgehend von diesem Zweckgedanken ist nicht nur die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift von Relevanz, sondern insbesondere die hierbei zugrundeliegende Technologie und deren Förderung.

Dank kryptographischen Verfahren soll für die elektronische Datenkommunikation nicht nur Verbindlichkeit, sondern - und insbesondere - auch Vertraulichkeit, Integrität und Authentizität gewährleistet werden. Die Kryptographie unterstützt damit zentrale Anliegen des Datenschutzes und der Datensicherheit.

Ob sich dies letztendlich auch praktisch umsetzen lässt, ist aufgrund des vorliegenden Entwurfes fraglich. Denn wenn Art. 10 BGES (wie im übrigen auch Art. 9 der eidgenössischen Verordnung vom 12. April 2000 über Dienste der elektronischen Zertifizierung, Zertifizierungsdiensteverordnung; ZertDV) aber lediglich festhält, die Zertifizierungsdienste müssten ihre Kunden spätestens bei der Ausstellung der elektronischen Zertifikate auf die Folgen eines möglichen Missbrauchs oder Verlustes des privaten Schlüssels aufmerksam machen, und sie müssten ihnen geeignete Massnahmen zur Geheimhaltung des privaten Schlüssels vorschlagen, offenbaren sich solcherlei Probleme. Dem nach Art. 16 BGES umfassend in die Pflicht genommenen Kunden sind die Abläufe in seinem Informatikumfeld in der Regel undurchschaubar. Eine geeignete Maßnahme zur Geheimhaltung des privaten Schlüssels könnte somit etwa darin gesehen werden, dass dem Kunden Komponenten (PC, Tastatur und Kartenleser) zur Verfügung gestellt würden, für die eine vertrauenswürdige Stelle - in der Regel wohl eine staatlich anerkannte Stelle - bestätigt, dass diese sicher arbeiten, insbesondere den privaten Schlüssel nicht kopieren. Da es solche Komponenten zur Zeit nicht gibt, fehlt es auch an staatlich anerkannten Bestätigungen. Ein verantwortungsbewusster Kunde wird - nicht zuletzt in Anbetracht der Beweislastumkehr nach Art. 17 BGES bei Missbrauch - von den ihm im Gesetz vorgeschlagenen Zertifikaten keinen Gebrauch machen.
Werden diese Einwände ernst genommen, ist zu einer generellen Verbreitung der digitalen Signatur aber vorab erforderlich, dass der Bund - wohl in Zusammenarbeit mit internationalen Gremien - benutzerfreundliche Technologien fördert und technische Komponenten zertifizieren hilft. Bereits eingeleitete Aktivitäten in diese Richtung (vgl. Projekt „guichet virtuel“) sind zu verstärken.

OW Aus der Sicht der Informatikverantwortlichen ist darauf zu drängen, dass die vielen noch offenen Fragen in Zusammenarbeit mit der Schweizerischen Informatikkonferenz (SIK) geklärt werden. Was den Datenschutz betrifft, verweisen wir auf die entsprechenden Bemerkungen der Kantone Bern und Zürich. Soweit das Grundbuch von den Erlassen betroffen ist, schliessen wir uns der Stellungnahme des eidgenössischen Amtes für Grundbuch- und Bodenrecht an.

SH Es erscheint uns richtig und wichtig, dass auf Gesetzesstufe die Voraussetzungen für einen sicheren Rechtsgeschäftsverkehr auf elektronischer Grundlage geschaffen werden. Damit wird die Möglichkeit geschaffen, Verträge elektronisch zu schliessen. Die mit der nötigen Sicherheitsinfrastruktur ausgebaute elektronische Signatur ist auch die unabdingbare Voraussetzung für den elektronischen Amtsverkehr der Bürgerinnen und Bürger mit den Amtsstellen. Angesichts der zunehmenden Bedeutung des Internets bzw. des E-Government stehen wir dem Entwurf daher grundsätzlich positiv gegenüber.

SG Wir befürworten die Schaffung einer formellen gesetzlichen Grundlage für die Anerkennung der Anbieterinnen von Zertifizierungsdiensten sowie die allgemeinen Bestimmungen über die Ausstellung und den Einsatz von elektronischen Signaturen. Wir halten die neuen Bestimmungen insbesondere auch darum für zweckmässig, weil sie für zukünftige technische Entwicklungen bzw. die Übernahme internationaler Standards in diesem Bereich offen sind.

SO Wir anerkennen das Bedürfnis nach der Einführung der elektronischen und digitalen Unterschrift für den Geschäfts- und den Privatverkehr per Internet. Grundsätzlich begrüssen wir, dass es inskünftig möglich sein soll, mit Hilfe der elektronischen Signatur Verträge abzuschliessen, für welche die schriftliche Form gesetzlich vorgeschrieben ist. Wichtig scheint uns, dass das vorliegende Gesetz die technischen Möglichkeiten nutzt und auf das Recht der Europäi-

schen Union (EU) abgestimmt ist. Die Wirtschaft ist auf die grenzüberschreitende rechtliche Anerkennung elektronischer Signaturen angewiesen. Wir beschränken unsere Vernehmlassung auf grundsätzliche Überlegungen. Weil uns das besondere Fachwissen fehlt, können wir zu den einzelnen Bestimmungen keine Stellung nehmen.

Rechtssicherheit: Die geltenden Allgemeinen Regeln des Obligationenrechts über die Entstehung der Obligation durch Vertrag wären auch auf die Verträge, die mit elektronischer Signatur geschlossen werden, anwendbar. Sie sind aber nicht auf die neuen Kommunikationstechnologien zugeschnitten. Das vorliegende Gesetz regelt in Art. 15a VE-OR ausschliesslich die Identifizierung der Personen, die auf elektronischem Weg Geschäfte abschliessen. Mangels Erfahrung in diesem jungen Rechtsgebiet fragen wir uns, wie die Vertragsparteien - bzw. im Streitfall die Gerichte - die besonderen Rechtsfragen lösen werden, die sich bei auf elektronischem Weg übermittelten und geschlossenen Verträgen stellen könnten. Wir denken dabei an Fragen wie: Wie wird der massgebliche Inhalt eines mit elektronischen Signaturen geschlossenen Vertrages bestimmt? Kann der Anbieter sicherstellen, dass das elektronisch signierte Angebot inhaltlich unverändert bei der Gegenpartei ankommt und von der Gegenpartei nicht verändert werden kann? Wann ist der Vertrag zustande gekommen? Welches ist die Form des Vertrages, auf welche im Geschäfts- und im Rechtsverkehr abzustellen ist? Ist es ausschliesslich die elektronische Form, wenn der Vertrag mit elektronischer Signatur abgeschlossen worden ist? In welcher Form muss der Vertrag aufbewahrt werden und wie kann sein Inhalt im Streitfall nach 10 oder 20 Jahren (subsidiäre Verjährungsfrist nach dem Vorentwurf des Bundesgesetzes über die Revision und Vereinheitlichung des Haftpflichtrechts) rechtsgenüglich nachgewiesen werden? Laut dem Begleitbericht (Seite 12) können auch einseitige empfangsbedürftige Willenserklärungen in digital signierter Form abgegeben werden. Hier fragt es sich, welche Voraussetzungen erfüllt sein müssen, damit solche Willenserklärungen als empfangen gelten und Rechtswirkung entfalten können.

Wir nehmen an, dass sich der Vertragsschluss mit elektronischer Signatur kaum durchsetzen wird, solange eine derartige Rechtsunsicherheit besteht.

SZ Wir können Ihnen mitteilen, dass wir gegen den Entwurf keine Einwendungen erheben.

TG Grundsätzlich ist zu begrüssen, dass der Abschluss von Rechtsgeschäften, für welche Schriftlichkeit notwendig oder vereinbart ist, auf elektronischem Weg ermöglicht wird. Auch wenn nur wenige Rechtsgeschäfte einem Formzwang unterliegen, wird die rechtliche Anerkennung und gesetzliche Regelung der digitalen Signatur ganz generell den Abschluss von Verträgen auf elektronischem Weg begünstigen. Dabei darf jedoch nicht ausser Acht gelassen werden, dass in Bereichen (z.B. Grundbuch), in welchen auf Grund der Tragweite des zugrundeliegenden Rechtsgeschäfts eine Beratung durch eine Amtsstelle an der Tagesordnung ist und deswegen auch besonders strenge Sorgfalts- und Verantwortlichkeitspflichten statuiert werden, der Einsatz von elektronischen Möglichkeiten - nicht zuletzt wegen der recht saloppen Handhabung derselben - sehr problematisch ist.

Im Übrigen bringt der Entwurf gegenüber der Verordnung über die Dienste der elektronischen Zertifizierung vom 12.04.2000 wenig Neues. Materiell bedeutsam und zu Bemerkungen Anlass geben jedoch die Revisionen des Zivilgesetzbuches und des Obligationenrechts.

TI La folgorante evoluzione della tecnica e il rapido sviluppo delle attività economiche e commerciali in forma elettronica richiedono precise norme legali, a tutela della sicurezza degli affari e degli utenti. Lo scrivente Consiglio concorda con l'opportunità di legiferare in questo settore e condivide di principio l'impostazione del progetto.
La proposta legislativa pone nondimeno diversi problemi di tipo tecnico, sui quali non è possibile esprimere valutazioni in considerazione della genericità del testo di legge, che dovrà in seguito essere precisato con disposizioni esecutive, la cui portata non può ancora essere valutata. Si pensi in particolare alla compatibilità dei diversi sistemi di crittografia e dei programmi, alla verifica e ai controlli dei requisiti di riconoscimento dei prestatori di servizi di certificazione, alla prestazione di servizi dall'estero, ai guasti tecnici ed informatici sempre possibili, e non da ultimo alla pirateria elettronica *(hackers)* che rende difficile garantire appieno la sicurezza delle transazioni elettroniche e virtuali.
Rivolgiamo pertanto la nostra attenzione essenzialmente ai problemi di tipo giuridico (in particolare la responsabilità per l'abuso delle firme elettroniche) e alle ricadute concrete che la nuova legislazione comporterà per i Cantoni e per gli utenti.

UR Die Vernehmlassungsvorlage betrifft das materielle und formelle Bundesrecht. Die gesetzliche Anerkennung der elektronischen Signatur drängt sich nicht zuletzt mit Blick auf die Entwicklungen im internationalen Umfeld geradezu auf. Die Anpassung der schweizerischen Gesetzgebung an die wirtschaftlichen und technischen Entwicklungen ist notwendig. Auch wenn der Regierungsrat des Kantons Uri deshalb die Vernehmlassungsvorlage vorbehaltlos unterstützt, verzichtet er auf die Ausarbeitung einer Vemehmlassung. Wie ein kantonsintern durchgeführtes Mitberichtsverfahren gezeigt hat, hat die Vemehmlassungsvorlage auf die Vollzugsorganisation des Kantons keine erheblichen Auswirkungen.

VD Le Conseil d'Etat vaudois est favorable au projet de loi fédérale sur la signature électronique, moyennant toutefois certains aménagements techniques. Il estime que l'assimilation de la signature électronique à la signature manuscrite répond à l'évolution de la technique dans les relations commerciales et du droit international privé. Le projet, qui s'entoure des garanties techniques et juridiques nécessaires pour attester de l'authenticité et de l'intégrité d'un document électronique et pour éviter un usage abusif de la signature électronique, répond à un besoin objectif et n'est pas critiquable dans son principe.
Le Conseil d'Etat vaudois estime qu'il est nécessaire de légiférer en matière de signature électronique afin de disposer d'une base légale formelle en la matière. Il constate que le projet reprend pour l'essentiel le contenu de l'ordonnance sur les services de certification électronique, entrée en vigueur le 1er mai 2000.
Une des innovations les plus importantes réside dans le nouvel art. 15a du Code des obligations. Cela se justifie dans la mesure où la signature électronique, qui permet de garantir l'authenticité et l'intégrité d'un document, semble offrir une sécurité au moins égale à celle de la signature manuscrite et qu'elle trouvera toujours plus d'applications à l'avenir.

VS Internet constitue un moyen privilégié pour l'échange d'informations entre particuliers, entreprises et administrations. Comme le souligne Michel Jaccard (Forme, preuve et signature électronique in Aspects juridiques du commerce électronique, Publications du Centre d'Etudes Juridiques Européennes - CEJE - Schulthess Zurich 2001 p. 113ss, p. 113) „Dans le domaine commercial, l'essor

du commerce électronique dépend largement de la confiance de ses utilisateurs dans la capacité de la technologie de transmettre de façon fiable, sûre et confidentielle les messages informatiques qui donneront lieu à des transactions commerciales. De plus, l'identification correcte de son partenaire contractuel et la garantie que les transmissions sont authentifiées et qu'elles reflètent effectivement la volonté de leurs auteurs sont essentielles“.
Dans ce contexte, la question de la signature électronique occupe une place centrale; de toute évidence, le projet de loi répond à un besoin avéré.
La LFSél. propose une telle infrastructure qui met aux prises trois acteurs et autant de relations juridiques. Pour l'essentiel, le projet reçoit l'aval du Conseil d'Etat qui comprend bien la nécessité d'opérer de nombreux renvois à une ordonnance du Conseil fédéral.

ZG Die Einführung der elektronischen Signatur für den rechtsgültigen Abschluss von Verträgen, welcher der einfachen Schriftform unterliegt, folgt einem Bedürfnis des heutigen digitalen Zeitalters, weshalb wir sie grundsätzlich begrüssen (Art. 15a E-OR). Auch den Ausbau des elektronischen Verkehrs mit Behörden bewerten wir grundsätzlich positiv.
Nach Ihrer Auffassung bietet die elektronische Signatur eine Sicherheit, welche jener der eigenhändigen Unterschrift überlegen ist. Zudem weisen Sie auf die lange Verfügbarkeit elektronischer Dokumente hin, warnen gleichzeitig aber auch davor, dass die Fälschungssicherheit im Verlauf der Zeit in erheblichem Mass sinkt. Grundsätzlich teilen wir Ihre Bedenken in Bezug auf die Fälschungssicherheit elektronischer Dokumente. Allerdings sind wir der Ansicht, dass sich die gleiche Problematik auch schon bei den herkömmlichen physischen Aufbewahrungsmethoden gestellt hat. Wir denken, dass sich mit der konsequenten Anwendung elektronischer Sicherheitsmassnahmen (Passworte, Verschlüsselung etc.) die Fälschungssicherheit auch in elektronischer Form bei längerer Aufbewahrungsdauer auf hohem Niveau sollte halten lassen können.
Zur generellen Verbreitung der digitalen Signatur ist vorab erforderlich, dass der Bund, wohl in Zusammenarbeit mit internationalen Gremien, benutzerfreundliche Technologien fördert und technische Komponenten zertifizieren hilft. Bereits eingeleitete Aktivitäten in diese Richtung sind zu verstärken, insbesondere auch für das Projekt „guichet virtuel“.

ZH Die Schaffung einer gesetzlichen Grundlage für den elektronischen Verkehr mit verschiedenen öffentlichen Registern wird begrüsst. Der Gesetzesentwurf ist ein taugliches und notwendiges Instrument, um die digitale Signatur auch in jenen (wenigen) Fällen anzuerkennen, in denen die Gesetzgebung bisher für einen gültigen Vertragsschluss eine handschriftliche Unterzeichnung verlangte. Hinsichtlich der Chancen einer weiten Verbreitung von digitalen Signaturen auf der Grundlage des vorliegenden Gesetzesentwurfs sind jedoch gewisse Zweifel anzubringen.
Im Licht der nachfolgenden Erwägungen wird der Gesetzesentwurf als grundsätzliche Anerkennung der neuen Technologie zwar begrüsst. Bei der Verwendung der digitalen Signatur stellt deren Gleichstellung mit der handschriftlichen Unterschrift aber lediglich die oberste und eher wenig verwendete Stufe dar. Viel häufiger und von entsprechend grösserer Bedeutung für den Geschäftsverkehr ist jedoch die Verwendung der digitalen Signatur etwa für Identifikation, sicheres E-Mailen oder den Abschluss formfreier Verträge. Auch hier besteht ein grosses Bedürfnis nach Wahrung der Integrität und Vertraulichkeit sowie Gewährleistung der Authentizität. Es ist daher sehr erwünscht,

dass der Bund benutzerfreundliche Technologien fördert und insbesondere auch einzelne technische Komponenten zertifizieren hilft (vgl. Tendenzen in diese Richtung beim Projekt „guichet virtuel“). Gerade im Hinblick auf die Einführung von Electronic Government ist die Förderung sicherer IT-Komponenten ein vordringliches Anliegen der Kantone.

Parteien / Partis / Partiti

CVP Die CVP Schweiz erachtet die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift als notwendig. Darum begrüsst sie auch die Schaffung eines Bundesgesetzes über die elektronische Signatur. Da der elektronische Geschäftsverkehr (E-Commerce) aus der heutigen wirtschaftlichen Welt nicht mehr wegzudenken ist, macht der Gesetzgeber einen Schritt in die richtige Richtung. Er passt das Recht an die technische Entwicklung an und schafft Rechtssicherheit. Die hier vollzogene rechtliche Gleichstellung macht den Geschäftsverkehr einfacher, schneller und sicherer, was für die betroffenen Wirtschaftsbereiche von Vorteil ist.

Die vorgeschlagenen rechtlichen Bestimmungen beschränken sich auf Fragen des Privatrechts. Im Verkehr mit Behörden (E-Government) bringt der Erlass keine wesentlichen Vorteile. Darum hat sich der Gesetzgeber die Frage zu stellen, ob er nicht auch in diese Richtung legiferieren sollte. Denn auch diese Entwicklung steht vor Tür oder hat die Schwelle in gewissen Bereichen bereits überschritten. Einzelne Mitglieder der CVP-Fraktion haben mit ihren parlamentarischen Vorstössen bereits mehrfach auf diese Notwendigkeit aufmerksam gemacht (99.3632 - Interpellation. Entwicklung zur Informationsgesellschaft. Wo bleibt die Schweiz?, NR Melchior Ehrler; 00.3028 - Interpellation. IT- und E-Commerce-Initiative, NR Peter Hess; 00.3057 - Motion. E-Commerce. Regulierungsbedarf, NR Adalbert Durrer; 00.3139 - Interpellation. Entbündelung des lokalen Zuganges, NR Melchior Ehrler). Das zeigt, dass die CVP solche Bestrebungen zumindest unterstützen würde.

FDP Die FDP Schweiz begrüsst den Erlass des vorliegenden Gesetzes, mit dem - neben anderem - im Privatrechtsverkehr die elektronische Signatur der eigenhändigen Unterschrift gleichgestellt wird. Vordringlich erscheint uns die beabsichtigte, möglichst rasche Inkraftsetzung dieses Gesetzes.

Bei der Umsetzung der Normen ist darauf zu achten, dass das BGES aber auch mit den international gebräuchlichen technischen Standards umgesetzt bzw. eingehalten werden kann. Schliesslich ist sicher zu stellen, dass die Umsetzung dieses Gesetzes selbst dann ohne Probleme erfolgen kann, wenn es in der Schweiz keine anerkannten CA's (Zertifizierungsdiensteanbieter) gäbe. Diesfalls sollten die schweizerischen Anerkennungsstellen verpflichtet werden, selbständig um die Anerkennung ausländischer CA's nachzusuchen.

Jungfreisinnige Einleitend ist zu sagen, dass die Jungfeisinnigen Schweiz mit dem Entwurf des BGES zufrieden sind. Wir unterstützen die Bemühungen des Bundesrates, im Bereich der digitalen Unterschrift eine Regelung zu erarbeiten. Wir bedauern sogar, dass es so lange gedauert hat. Es ist absolut notwendig, dem elektronischen Geschäftsverkehr eine rechtliche Grundlage zu geben, die es erlaubt, Verträge im privatrechtlichen Sinn über das schon weit verbreitete und stark benutzte verwendete Medium E-Mail abzuschliessen. Dadurch werden etliche Prozesse der Geschäftswelt erleichtert. Des weiteren wird das Risiko für Händler und Käufer verkleinert. Die Geschäftsbeziehung kann nachgewiesen werden. Vor allem die Händler haben nun ein Instrument in der Hand, mit dem sie ihr, zum realen Geschäftsablauf um einiges grössere Risiko

verringern können. Als dritter Hauptpunkt für die Einführung einer durch ein formelles Gesetz geregelte digitale Signatur ist der Vertrauensgewinn in das Medium Internet. In letzter Zeit häuften sich die Meldungen über Betrügereien im Internet. Es gibt noch immer etliche Personen, die dem Internet nicht trauen und deshalb die Hände vom E-Commerce lassen.

PLS En guise de préambule, nous souhaitons insister sur le fait que le Parti libéral se déclare favorable à ce projet de loi qui permettra à la Suisse de disposer, dans le domaine de la signature électronique, d'une réglementation comparable à celle de ses principaux partenaires commerciaux. L'instauration par la loi d'une équivalence entre la signature manuscrite et la signature électronique fondée sur une certification sera de nature à permettre le développement du commerce électronique dans un cadre juridique bien défini.

SVP Die SVP geht mit dem Bericht einig, dass die Abwicklung von rechtsgeschäftlichen Vorgängen auf elektronischem Wege weiter zunehmen. Die SVP spricht sich daher für den vorgeschlagenen Gesetzesentwurf aus. Wesentlich ist dabei, dass die elektronische Signatur einen Schutz erhält und in gleichem Masse wie die eigenhändige Unterschrift Rechtssicherheit gewährleistet.

Der Bedarf an einer gesetzlich anerkannten elektronischen Signatur wird längerfristig gross sein. Für die SVP ist die Frage der Rechtssicherheit von grosser Bedeutung. Wer eine mit einer anerkannten Signatur versehene Vertragserklärung erhält, hat nicht dieselbe Gewissheit auf Verbindlichkeit wie im Falle einer eigenhändig unterzeichneten Erklärung. Ausgleich bietet die Haftung des Signaturinhabers (Art. 17 Abs. 2). Es ist eine Beweislastumkehr vorgesehen. Der Signaturinhaber und nicht sein vermeintlicher Geschäftspartner muss im Streitfall beweisen, dass der geheime Signaturschlüssel ohne den „Willen" des Inhabers zum Einsatz gekommen ist.

Heute ist der echte Bedarf im Vertragsrecht sowohl wirtschaftlich wie rechtlich noch gering, da die meisten Geschäfte bereits online abgewickelt werden können (z.B. Internet-Bank, Online-Shopping). Geschäfte unter Firmen sowie der Verkehr mit Behörden werden relevante Anwendungsbereiche sein. Online-Shopping von Verbrauchern spielt sich heute schon ohne elektronische Unterschrift ab. Der Konsument hat keinen Anlass, die elektronische Unterschrift zu benützen, da er sich damit nur eine strengere Haftung einhandelt.

Organisationen / Organisations / Organizzazioni

Briner Unsere Bemerkungen sind, dem Zweck einer Vernehmlassung entsprechend, im wesentlichen alle kritisch, und wir möchten daher gerne voranstellen, dass der Entwurf in seiner Konzeption und seinen Grundlinien überzeugt, auch mit seiner klaren Einbettung in den von der EU gezogenen Rahmen, und nicht zuletzt mit dem vorgesehenen straffen Zeitplan. Allerdings ist die Vernehmlassungsfrist sehr kurz, und wir halten dafür, dass die um einen Monat längere Vernehmlassungsfrist zur OR- und UWG-Revision ohnehin abgewartet werden muss.

camera commercio Avantutto cogliamo l'occasione per confermare quanto già ripetutamente detto in altre sedi, ossia che la questione di una regolamentazione legale della firma digitale riveste un'importanza fondamentale per gli operatori economici ed è importante che la Svizzera non rimanga troppo in ritardo rispetto all'Unione europea, che si è già dotata di importanti strumenti legali.

CP Nous relevons en préambule que par le biais la signature électronique, on dispose d'un procédé technique qui permet de déterminer l'origine du document électronique (authenticité) et l'on est à même de vérifier que le document est

resté inchangé (intégrité). La signature a donc une double fonction et garantit une meilleure sécurité que la signature manuscrite. Il paraît donc normal de la consacrer dans notre droit et d'inclure un article à ce sujet dans le Code des obligations.

Nous pensons que le projet de loi est dans l'ensemble bien orienté. Cependant, nous estimons que la distinction entre les organismes de reconnaissance, les organismes d'accréditation, ceux de surveillance est tout sauf claire. Il nous paraît important de revoir ce point.

Distefora Die Vorlage trägt dem veränderten Umfeld der modernen Informationsgesellschaft und den neuen Vertriebswegen im Bereich des E-Business Rechnung, wobei die Gleichstellung der elektronischen Signatur mit der handschriftlichen Unterschrift sicherlich ein wesentlicher Baustein für einen nachhaltigen Durchbruch des E-Commerce darstellt. Bestehende Rechtsunsicherheiten im elektronischen Geschäftsverkehr werden durch die Vorlage zumindest teilweise beseitigt, weshalb ein rasches Inkrafttreten der Vorlage sehr zu begrüssen ist.

DSB Das Büro von DSB+CPD. CH hält den Entwurf für ein taugliches und notwendiges Instrument, um die digitale Signatur auch in den seltenen Fällen zum Einsatz gelangen zu lassen, wo die Gesetzgebung bisher zu einem gültigen Vertragsschluss eine handschriftliche Unterzeichnung verlangte.

Das Gesetz gibt damit einen Hinweis, dass die für digitale Signaturen generell vorgesehene Technologie hohen Ansprüchen genügen könnte. Gemäss seinem Art. 1 bezweckt es denn auch die Förderung eines breiten Angebotes an sicheren Diensten der elektronischen Zertifizierung. Ausgehend von diesem Zweckgedanken ist aus Sicht des Datenschutzes nicht nur die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift von Relevanz, sondern auch (oder gerade) die hierbei zugrundeliegende Technologie und insbesondere deren Förderung. Der Einsatz und die Verbreitung der Kryptographie sind wichtige Postulate des Datenschutzes. Dank kryptographischen Verfahren kann für die elektronische Datenkommunikation nicht nur Verbindlichkeit, sondern auch Vertraulichkeit, Integrität und Authentizität gewährleistet werden. Die Kryptographie unterstützt also zentrale Anliegen des Datenschutzes und der Datensicherheit.

Wenn Art. 10 BGES – wie die aktuelle Zertifizierungsdiensteverordnung – aber einzig festhält, die Zertifizierungsdienste müssten ihre Kunden spätestens bei der Ausstellung der elektronischen Zertifikate auf die Folgen eines möglichen Missbrauchs oder Verlustes des privaten Schlüssels aufmerksam machen und sie müssten ihnen geeignete Massnahmen zur Geheimhaltung des privaten Schlüssels vorschlagen, zeigen sich die Probleme der praktischen Umsetzung in deutlicher Weise: Dem nach Art. 16 BGES umfassend in die Pflicht genommenen Kunden sind die Abläufe in seinem Informatikumfeld in aller Regel völlig undurchschaubar. Eine geeignete Maßnahme zur Geheimhaltung des privaten Schlüssels könnte somit etwa darin gesehen werden, dass dem Kunden Komponenten (PC, Tastatur und Kartenleser) zur Verfügung gestellt würden, für die eine vertrauenswürdige Stelle – in der Regel wohl eine staatlich anerkannte Stelle – bestätigt, dass diese sicher arbeiten, insbesondere den privaten Schlüssel nicht kopieren. Da es solche Komponenten zur Zeit nicht gibt, fehlt es auch an staatlich anerkannten Bestätigungen. Ein verantwortungsbewusster Kunde wird – nicht zuletzt in Anbetracht der Beweislastumkehr nach Art. 17 BGES bei Missbrauch – von den ihm im Gesetz vorgeschlagenen Zertifikaten

keinen Gebrauch machen. Die heute schon – ohne gesetzliche Anerkennung – zur Verfügung stehenden Zertifikate werden ihm bessere Dienste leisten.
Für die Kantone bedeutet dies, dass sie zur Einführung von e-government in ihren Erlassen - beispielsweise zur Gültigkeit einer elektronischen Eingabe aber auch für den elektronischen Informationsaustausch zwischen Behörden und Bürgern - nicht auf die Lösung des BGES zurückverweisen dürfen. Die vom BGES ausgehenden Impulse bestehen daher in erster Linie in der grundsätzlichen Anerkennung der eingesetzten Technologie und - allenfalls in einer späteren Phase - in den durch Bundesrats- oder Departementsverordnungen ausgehenden Technologieregelungen tieferer Stufe.
Die gesetzliche Regelung steht dem technologischen Fortschritt aber insgesamt - was durchaus positiv zu vermerken ist - nicht im Weg. Zur generellen Verbreitung der digitalen Signatur ist jedoch vorab erforderlich, dass der Bund - wohl in Zusammenarbeit mit internationalen Gremien - benutzerfreundliche Technologien fördert und technische Komponenten zertifizieren hilft. Bereits - etwa im Projekt „guichet virtuel“ - eingeleitete Aktivitäten in diese Richtung sind zu verstärken. Gerade aus Sicht des Datenschutzes muss diese Forderung mit Nachdruck erhoben werden: Wird mit der digitalen Signatur die handschriftliche Unterschrift bei Vertragsschlüssen ersetzt, bildet dies gleichsam den „oberen Abschluss“ des Einsatzumfelds der digitalen Signatur. Viel häufiger und wichtiger wird der Einsatz der digitalen Signatur aber zur Identifikation oder für sicheres E-Mail und zum Abschluss formloser Verträge sein. Hier wird sie - wie bereits erwähnt - zu einem zentralen Instrument des Datenschutzes. Aus Sicht der Kantone ist es daher vordringlicher, dass ihr hier durch die Förderung sicherer Komponenten zum Durchbruch verholfen wird. Der Gesetzesentwurf bietet Gelegenheit, dies in Erinnerung zu rufen.

economiesuisse Mit der heutigen Vorlage wird einem langjährigen Anliegen der Schweizer Wirtschaft Rechnung getragen. Wir begrüssen es, dass mit der vorgenommenen Aufteilung der Vorlage rasch die Gleichstellung der elektronischen Signatur mit der handschriftlichen Signatur auf Gesetzesstufe geregelt werden kann. Damit wird ein wichtiges klares Zeichen zugunsten der Entwicklung der Informationsgesellschaft in der Schweiz gesetzt, auch als notwendige Voraussetzung für das E-Government.
Entsprechend begrüssen wir mit unseren Mitgliedorganisationen die Vorlage klar. Wir erwarten, dass sie möglichst auf den 1. Januar 2002 in Kraft gesetzt wird. Wir sind überzeugt, dass die betreffenden parlamentarischen Beratungen speditiv vorangetrieben werden, und werden unsererseits entsprechend Einfluss nehmen. Dispute über technische Bereinigungen dürfen nicht zu einer Verzögerung führen, doch müssen die angesprochenen Probleme unter Einbezug der Erfahrungen aus der Praxis gelöst sein.
Für die Entwicklung von spezifischen Software-Angeboten und die Bereitstellung von neuen Internetdienstleistungen ist die Klarstellung der rechtlichen Rahmenbedingungen notwendig und dringend. Diese Produkte werden zur Zeit breit entwickelt und in den nächsten Monaten auf dem Markt verfügbar werden. Die Schweiz darf hier nicht weiter in Rückstand zu den Konkurrenzländern geraten. Entsprechend ist die rasche Verabschiedung von grosser Bedeutung. Es ist richtig, dass die Vorlage sich auf diese technische Gleichstellung konzentriert und nicht eine grundsätzliche Änderung des Vertrags- und des Stellvertretungsrechts damit vermengt. Mit der Abstützung der Vorlage auf die heutige Zertifizierungsvorlage und der Abtrennung der übrigen Anpassungen

des Obligationenrechts und des UWG wurden dafür gute Voraussetzungen geschaffen.
Zusammenfassend kann sodann auch festgehalten werden, dass wir es ausserordentlich begrüsst hätten, wenn das Gesetz voll zur EU-Richtlinie kompatibel und technologieneutral formuliert wäre. Auch ist es zwingend erforderlich, dass die Ausführungsbestimmungen gleichzeitig mit dem Gesetz in Kraft treten, namentlich angesichts des hohen Stellenwertes im heutigen Konzept. Zu den Ausführungsvorschriften sind in jedem Fall die betroffenen Kreise wie auch die Spitzenorganisationen zu konsultieren.

EKK Il est important qu'une base légale soit créée dans ce domaine pour suppléer à l'ordonnance expérimentale limitée dans le temps qu'est l'ordonnance sur les services de certification. La future loi fédérale sur la signature électronique ne pourra ainsi qu'apporter une sécurité juridique supplémentaire dans ce domaine technologique de pointe.

FHZ Das Gesetz ist sinnvoll, gut gestaltet und deckt die Bedürfnisse ab. Es ist wichtig, dass das Gesetz ohne Verzug in Kraft gesetzt wird. Die entsprechenden Verordnungsbestimmungen sollten auch ohne Verzug, d.h. mit diesem Gesetz in Kraft treten. Es ist aktuell, wie auch in Zukunft sicherzustellen, dass das Gesetz mit internationalen technischen Standards umgesetzt resp. eingehalten werden kann. Es ist sicherzustellen, dass das Gesetz auch problemlos umgesetzt werden kann, falls es keine schweizerischen CA gibt, resp. gäbe.

FRC Nous approuvons la proposition de rendre équivalentes, pour tous les contrats de droit privé, la signature électronique et la signature manuscrite.
Il est évident qu'en matière de commerce électronique il existe un déséquilibre technologique et informatif entre les fournisseurs et les consommateurs. Il est tout aussi évident que les documents électroniques sont lus avec moins d'attention que les dispositions figurant sur papier.
Nous demandons donc que les consommateurs soient informés très complètement des chances mais aussi des risques liés à la signature électronique et nous estimons que, de ce point de vue, le présent projet doit être complété.

FRI Sur un plan général, nous souscrivons pleinement à l'objectif du projet de loi sur la signature électronique qui vise à assimiler la signature électronique à la signature manuscrite, permettant ainsi la conclusion contractuelle par voie électronique.
Notre ordre juridique se doit, en effet, de suivre l'évolution technologique, notamment en matière de droit des contrats. Le fait qu'un procédé technique permette, d'une part, de déterminer l'origine du document électronique et de garantir, d'autre part, que son contenu n'a pas été modifié est de nature à nous rassurer pleinement. Ces notions d'authenticité et d'intégrité confèrent à la signature électronique une sécurité accrue par rapport à la signature manuscrite traditionnelle envoyée par courrier.
Il nous paraît également urgent de remplacer, par une législation adéquate, l'actuelle ordonnance sur les services de certification qui présente d'importantes lacunes, notamment au niveau de la responsabilité du titulaire des clés et des fournisseurs de services de certification.

FSP Nous observons que le projet de loi fédérale sur la signature électronique soulève, sans y répondre, un certain nombre d'interrogations, relatives notamment à la définition (peu claire) de la forme requise pour certains actes juridiques et à l'étendue des compétences des autorités de surveillance ; que, de surcroît, l'application de cette loi exigera la mise en place d'une importante bureaucratie

et de mesures techniques coûteuses, dont l'efficacité n'est de loin pas démontrée.

C'est pourquoi notre Fédération, si elle est favorable au principe de l'adoption d'une loi fédérale en la matière, considère néanmoins que les modalités de sa mise en application sont de nature à créer des problèmes supplémentaires. Elle doit donc être renvoyée à leurs auteurs pour réexamen.

Notre Fédération est favorable au principe de l'adoption de la loi fédérale sur la signature électronique, mais souhaite que les modalités de la mise en œuvre de ladite loi soient davantage précisées.

ISACA L'ISACA salue la mise en place de cette législation qui devrait permettre de développer harmonieusement ce domaine en Suisse.

L'ISACA regrette que cette nouvelle législation se limite en principe au droit privé. Il serait en effet souhaitable de pouvoir étendre ces règles à l'ensemble de la cyberadministration afin d'éviter notamment la prolifération de mécanismes de certification à l'échelon des cantons et des communes.

kf Grundsätzlich begrüsst das Konsumentenforum kf deutsche Schweiz, dass die elektronische Signatur der handschriftlichen gleichgestellt wird und unterstützt das Bemühen einer rasch möglichen Einführung. Aus diesem Grunde hoffen wir, dass die noch etwas vage formulierten Haftungsfragen noch genauer in begleitenden Vorschriften geregelt werden.

KPMG Die geltenden Formvorschriften tragen der Entwicklung des modernen Rechtsverkehrs nicht mehr ausreichend Rechnung. Globalisierung, Mobilität des Handelns, technologische Entwicklung haben zur Folge, dass heute eine Vielzahl von Erklärungen praktisch zeitverzugs- und kostenlos über enorme Distanzen abgegeben werden können. Unter diesen Bedingungen behindert die heutige Schriftform, die unter den vorgesehenen Formvorschriften die Gängigste ist, einen rationellen und wirtschaftlichen Einsatz neuer Kommunikationstechniken. Im Interesse des Wirtschaftsstandorts Schweiz und der Rechtssicherheit begrüssen wir deshalb grundsätzlich die Schaffung von juristischen Rahmenbedingungen zur vermehrten Nutzbarmachung des Internets für kommerzielle Wirtschaftsvorgänge. Dazu gehört auch der Erlass von Rechtsnormen, die dazu beitragen, dass elektronische Signaturen als sicher gelten und Fälschungen digitaler Signaturen zuverlässig festgestellt werden können. Ferner begrüssen wir auch die mit dem neuen Art. 15a des Obligationenrechts verfolgte Möglichkeit, das Formerfordernis gemäss Art. 14 OR anhand einer elektronischen Signatur erfüllen zu können.

An dieser Stelle möchten wir nochmals darauf hinweisen, dass die allgemeine Akzeptanz der elektronischen Signatur ein wichtiges Ziel der neuen Gesetzgebung sein muss. Vom allgemeinen Vertragsrecht abweichende Normen sollten aufs absolut Notwendige beschränkt und nur dort aufgestellt werden, wo sich aufgrund der materiellen Unterschiede auch rechtliche Sondernormen aufdrängen. Schliesslich werden die Vertragsparteien entscheiden, ob und auf welche Art und Weise Willenserklärung in Zukunft signiert werden.

Ein weiterer wichtiger Punkt scheint uns die Vereinbarkeit der schweizerischen E-Signatur-Gesetzgebung mit dem europäischen Recht bzw. mit dem entsprechenden Recht der EU-Mitgliedstaaten. In einem internationalen Rechtsgebiet wie dem elektronischen Rechtsverkehr sollten schweizerische Sondernormen unter allen Umständen vermieden werden.

Kunststoffverband Normalerweise schätzen wir möglichst lange Vernehmlassungsfristen. In diesem Fall ist jedoch die verkürzte Frist zu begrüssen, kann doch so das Parlament bereits in der Juni-Session darüber befinden. Für einmal wurden

hier die Bedürfnisse der Wirtschaft berücksichtigt, ist diese doch dringend darauf angewiesen, den diesbezüglichen Rückstand zum Ausland raschmöglichst aufzuholen. Wünschbar wäre, das Gesetz per 1.1.2002 in Kraft zu setzen.
Materiell haben wir zum - absolut notwendigen - Gesetzesentwurf keine Bemerkungen, behandelt er doch etwas, was im Geschäftsverkehr schon fast Standard geworden ist und deshalb dringend einer gesetzlichen Regelung bedarf.

KVN Einleitend stellen wir fest, dass mit der Anerkennung der elektronischen Signatur ein wichtiger Grundstein für den elektronischen Geschäftsverkehr der Zukunft gelegt wird. Damit kann die Schweiz rechtzeitig mit den rechtlichen Regelungen ausgerüstet werden.
Eine genauere Prüfung zeigt jedoch, dass eine solche Regelung für die Konsumenten weitreichende Konsequenzen hat. Die zusätzlichen Haftungsrisiken bringen vorerst nur Nachteile, deshalb sollte darauf hingewiesen werden, dass auch inskünftig in vielen Bereichen, wie z.B. im Internet-Shopping, der Gebrauch einer digitalen Signatur nach wie vor überflüssig ist. Im weiteren ist es aus diesen Gründen auch unumgänglich, bei Nutzungsbeschränkungen einer Signatur klare Standards zu schaffen, damit jegliche Rechtsunsicherheit eliminiert werden kann.

Landestop Die Vorlage erscheint uns im Hinblick auf die tatsächlichen Verhältnisse, bzw. den heutigen Bedürfnissen der Praxis, angebracht und sinnvoll.

Rosenthal Die vorliegende Stellungnahme beschränkt sich auf die Frage der Rechtswirkung der elektronischen Signatur (fortan Signatur) und der Haftung nach Art. 17 und 18 BGES-VE. Diese scheinen dem Verfasser dieser Stellungnahme nicht genügend klar und sauber geregelt. Überdies schafft die derzeitige Fassung des BGES nicht die Rechtssicherheit, die beim Einsatz von Signaturen nach Ansicht des Verfassers erforderlich ist.
Damit soll der BGES-VE nicht grundsätzlich in Frage gestellt werden. Es ist zu begrüssen, dass ein schlankes Gesetz realisiert werden konnte, anhand dessen die Fragen zur Rechtswirkung der Signaturen diskutiert werden können. Auch mussten „historische“ Gegebenheiten wie die bereits vorliegende Zertifizierungsdiensteverordnung (ZertDV) berücksichtigt werden, was den Handlungsspielraum einschränkt. Der Verfasser der Stellungnahme geht denn auch davon aus, dass sich die nachfolgend angeführten Mängel durch eine Überarbeitung der genannten Artikel beheben lassen. Konkrete Formulierungsvorschläge sind dem Verfasser im Rahmen seiner persönlichen Stellungnahme aus zeitlichen Gründen nicht möglich.
Das BGES wird zweifellos die Akzeptanz der Signatur als interessantes „Instrument“ im elektronischen Geschäfts- und Behördenverkehr steigern. Der Verfasser geht jedoch nicht davon aus, dass in den kommenden Jahren bei einem breiteren Publikum ein echtes Bedürfnis nach staatlich anerkannten Signaturen vorhanden sein wird. Euphorie oder übertriebene Erwartungen sind fehl am Platze; sie führen nur zu Enttäuschungen, was dem gesamten Vorhaben schaden würde.
Der Verfasser vertritt in dieser Stellungnahme seine persönliche Auffassung und handelt nicht in fremden Auftrag oder Vertretung fremder Interessen.

SBB Die SBB begrüssen die Vorlage (ebenso wie den Entwurf eines Bundesgesetzes über den elektronischen Geschäftsverkehr) sehr; sie schliesst eine wichtige Lücke, welche sich infolge der schnellen technischen Entwicklung auf diesem Gebiet je länger je mehr gezeigt hat. Wir plädieren dafür, dass die beiden Vor-

lagen angesichts dieser rasanten Entwicklung dringlich behandelt werden, damit diese rasch verabschiedet werden können.

SBV Notre Association approuve le projet de loi, qui permet à la Suisse de se doter, dans le domaine des certificats numériques, d'une réglementation-cadre comparable à celle de ses principaux partenaires commerciaux. En consacrant l'équivalence entre la signature manuscrite et la signature électronique fondée sur un certificat qualifié, le projet de loi est par ailleurs de nature à susciter la confiance du Public et par conséquent à stimuler le développement du commerce électronique.

La réglementation proposée ne donne toutefois pas d'indications particulières sur la création des signatures électroniques. Ainsi, la notion de „dispositif sécurisé de création de signature électronique“, qui revêt un rôle essentiel dans la directive européenne sur les signatures électroniques, ne figure pas dans la loi. Il s'agit d'une lacune importante à laquelle il convient de remédier. Cela d'autant plus que, selon la directive, seules les „signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature“ répondent en principe aux exigences légales d'une signature manuscrite. Il nous paraîtrait essentiel d'assurer, dans ce domaine, la compatibilité entre les droits suisse et européen.

Cette lacune paraît d'autant plus problématique que le fournisseur de services de certification, qui n'a en principe pas pour tâche de créer des signatures électroniques, est tenu, selon le projet de loi, d'indiquer aux titulaires de certificats électroniques „les mesures appropriées pour maintenir leur clé privée secrète“. Or, ces indications ont une incidence déterminante sur l'obligation de diligence du titulaire de la clé privée et, par conséquent, sur la responsabilité encourue par ce dernier en cas d'utilisation abusive de sa clé. L'étendue du devoir de diligence à la charge du titulaire de la clé privée devrait donc être précisée, à tout le moins dans l'ordonnance ou dans les prescriptions d'exécution de la loi.

SGB Wir begrüssen es, dass der Bundesrat mit dem vorgeschlagenen Gesetz die Voraussetzung dafür schafft, dass künftig Verträge, für die die Schriftform erforderlich ist, auch auf elektronischem Weg abgeschlossen werden können. Zu den vorgeschlagenen formellen und materiellen Regelungen des Gesetzes haben wir keine Bemerkungen.

Schlauri/Kohlas Der Vorentwurf für ein Bundesgesetz über elektronische Signaturen soll nebst einer sauberen gesetzlichen Grundlage für eine Public-Key-Infrastruktur nun auch die prozess- und zivilrechtliche Anerkennung der digitalen Signatur bringen sowie die entstehenden Haftungsfragen klären. Die Regelung dieser Aspekte ist grundsätzlich zu begrüssen, weil durch sie einer Technologie der juristische Weg frei gemacht wird, die im elektronischen Geschäftsverkehr einige Bedeutung erlangen dürfte.

SfK Grundsätzlich begrüsst die Stiftung für Konsumentenschutz, dass die elektronische Unterschrift der handschriftlichen Signatur rechtlich gleichgesetzt wird. Dies wird kurzfristig vor allem Auswirkungen auf das Business-to-Business-Geschäft haben, langfristig werden sich auch für KonsumentInnen neue Chancen eröffnen. Aber auch Risiken.

Gerade im E-Commerce besteht oft ein technologisches und informatives Ungleichgewicht zwischen Anbieter und Verbraucher. Die meisten KonsumentInnen sind sich zudem zuwenig bewusst, dass auch ein simpler Mausklick Rechtsfolgen mit sich bringen kann. Und es ist eine Tatsache, dass elektronische Dokumente unsorgfältiger gelesen werden als solche auf Papier.

Die oft äusserst einseitigen Haftungsbeschränkungen zu Lasten der KonsumentInnen sind ein Zeichen dafür, dass sich selbst Online-Anbieter dem Medium Internet oft nicht sicher sind (ein glänzendes Beispiel dafür sind die einseitigen Haftungsbedingungen im Onlinebanking). Auch sind uns die meisten E-Commerce-Anbieter nicht gerade durch eine offene und transparente Geschäftspolitik aufgefallen. Darum erachten wir es als wichtig, dass in diesem wichtigen Bereich der digitalen Signatur Richtlinien geschaffen werden, durch welche die KonsumentInnen vollumfänglich über die Chancen und vor allem auch Risiken der elektronischen Unterschrift aufgeklärt werden.
Während die Bedeutung einer handschriftlichen Signatur den meisten KonsumentInnen klar sein dürfte und mit entsprechender Sorgfalt und Zurückhaltung eingesetzt wird, muss für die digitale Unterschrift noch ein Prozess in Gang gesetzt werden, damit die KonsumentInnen auch damit einen sorgfältigen Umgang pflegen und sich den Rechtsfolgen eines Mausklicks bewusst werden.

SICTA Wir begrüssen es, dass der Bund in diesem Bereich den Handlungsbedarf erkannt hat und sind zuversichtlich, dass damit eine gesetzliche Regelung in Kraft gesetzt wird, die den wirtschaftlichen Bedürfnissen in Bezug auf den elektronischen Geschäftsverkehr gerecht wird.
Die Schweiz muss sich in diesem Bereich rasch dem EU-Recht anpassen und die gegenseitige Anerkennung der Zertifikate gewährleisten, denn nur ein europaweiter rechtlicher Rahmen vermag das gegenseitige Vertrauen in digitale Signaturen zu schaffen und damit den elektronischen Geschäftsverkehr und die elektronische Kommunikation weltweit zu fördern. Das Europäische Parlament hat denn auch eine recht liberale Lösung gewählt: Es wurden nur grundlegende und relativ allgemein gehaltene Anforderungen an Zertifikate und Zertifizierungsdiensteanbieter formuliert; den Mitgliedstaaten wird offen gelassen, auf freiwilliger Basis Akkreditierungsregelungen auf der Grundlage gemeinsamer Anforderungen zu erlassen.
Nach der Verabschiedung einer entsprechenden Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen durch das Europäische Parlament, erliess die Schweiz in einem ersten Schritt zur Förderung der digitalen Signatur die Verordnung über die Dienste der elektronischen Zertifizierung. Vergleicht man die Erlasse anderer Staaten wird ersichtlich, dass praktisch sämtliche Länder eine Lösung auf Gesetzesstufe eingeführt haben. Mit diesem Gesetz schafft nun auch die Schweiz eine klare rechtliche Grundlage für die Gleichstellung der digitalen Signatur mit der handschriftlichen Unterschrift. Damit wird einem langjährigen Anliegen der Schweizer Wirtschaft Rechnung getragen. Die SICTA begrüsst es, dass damit ein klares Zeichen zugunsten der Entwicklung der Informationsgesellschaft in der Schweiz gesetzt wird.
Zusammenfassend unterstützt die SICTA den vorgelegten Entwurf und stellt hiermit folgenden Antrag: Es sollte seitens des Bundes alles unternommen werden, damit die Vorlage in dieser Form möglichst rasch in Kraft gesetzt werden kann.

SIK Zuerst möchten wir betonen, dass wir es sehr begrüssen, dass der Gesetzgeber in diesem zukunftsträchtigen Bereich (endlich) aktiv wird. Auch die Einfachheit und Übersichtlichkeit der Entwürfe beeindrucken uns, insbesondere die offensichtliche Absicht, den Text möglichst unabhängig von der Technik und ihrer Entwicklung zu halten.

SUISA Als Urheberrechtsgesellschaft, die in einem weltweiten und weitverzweigten Netz eingebunden ist und für die die elektronische

Geschäftstätigkeit eine rasch zunehmende Bedeutung erlangt hat, begrüssen wir das Gesetzesvorhaben sehr und sind auch mit dessen allgemeiner Stossrichtung einverstanden.

Dass elektronische Kommunikation wie keine andere vorher grenzüberschreitend ist, bedarf keiner weiteren Ausführungen. Von da her ist die internationale Harmonisierung der rechtlichen Vorschriften hier so zentral wie wohl in keinem anderen Bereich. Das bedeutet, dass die schweizerische Gesetzgebung nur aus absolut zwingenden Gründen vom europäischen Recht abweichen sollte.

swisscom Wir begrüssen den Entwurf insgesamt und die Absicht, auch die materiellrechtliche Seite der elektronischen Signatur zu regeln. Dem Gesetz kommt Signalwirkung zugunsten der Förderung der Informationsgesellschaft in der Schweiz zu.

Swisscom hat sich in den letzten Jahren intensiv mit Fragen der digitalen Signatur auseinandergesetzt und auch bei der Erarbeitung der Zertifizierungsdiensteverordnung mitgewirkt. Da wir die Vorlage insgesamt als ausgewogen erachten, verzichten wir auf eine detaillierte Stellungnahme zu einzelnen Punkten. Dennoch sind wir uns bewusst, dass einzelne Punkte des BGES in der Praxis zu diskutieren geben werden. Zu denken ist insbesondere an die Haftungsnormen (Art. 17 und 18 VE).

SwissITC Wir sind daran interessiert, dass die Vorlage so rasch wie möglich umgesetzt wird. Für die ICT Branche wird damit ein klares Zeichen zur Verbesserung der Marktbedingungen gesetzt, denn mit der Gleichstellung von elektronischer Signatur und handschriftlicher Unterschrift werden die vorhandenen Rechtsunsicherheiten beseitigt.

Swisskey Die Vorlage trägt den langjährigen Anliegen der Schweizerischen Wirtschaft Rechnung, weshalb wir die Vorlage grundsätzlich begrüssen. Es ist wesentlich für den Durchbruch des E-Business, dass die elektronische Signatur der handschriftlichen Unterschrift gleichgestellt wird. Dies ist ein klares Zeichen auf dem Wege zur Informationsgesellschaft bzw. auch zum E-Government und bildet einen wichtigen Schritt dahin. Es werden Rechtsunsicherheiten, die im elektronischen Geschäftsverkehr bestehen, zum Teil beseitigt. Ein rasches Inkrafttreten eines Bundesgesetzes ist zu begrüssen.

EU-Kompatibilität

Die wichtigste Forderung an das Bundesgesetz über die elektronische Signatur muss die Kompatibilität mit der europäischen Rechtsetzung sein. Der vorliegende Entwurf ist nicht EU-kompatibel. Dies wird aber ausdrücklich gefordert. Sowohl die EU als auch die Nachbarländer verfügen über gesetzliche Regelungen zur digitalen Signatur. Die EU hat am 13. Dezember 1999 eine Richtlinie zur Vereinheitlichung der Anforderungen an die Zertifizierdiensteanbieter und an die digitale Signatur erlassen. Die Schweiz kann sich diesen Regeln nicht entziehen. Insbesondere fehlen im vorliegenden Entwurf klare Regeln zur Anerkennung von Signaturen im internationalen Kontext. Es fehlt eine automatische Anerkennung der in der EU zugelassenen Anbieter von Zertifizierungsdiensten, welche die EU-Richtlinie erfüllen. Gerade im elektronischen Geschäftsverkehr werden langfristig die nationalen Grenzen verschwinden und daher darf ein solches Gesetz nicht nationalen Charakter aufweisen. Neue Gesetze müssen diese Anforderung erfüllen und auch auf die internationale Situation abgestimmt werden. Es sind keine Insellösungen gefragt, ansonsten die internationale Zulassung von Anbietern in der Schweiz verunmöglicht wird bzw. mit enormen Kosten zur Erlangung der Anerkennung im Ausland verbunden ist.

Technisch neutral

Die EU in ihrer Richtlinie und die verschiedenen Mitgliedstaaten in ihren nationalen Gesetzen über die digitale Signatur haben es vorgemacht und den Text technisch neutral - also offen für zukünftige neue Technologien - abgefasst. Ein Signaturgesetz sollte alle möglichen Verfahren beinhalten und keines ausschliessen. Dies wäre auch für das Bundesgesetz wünschenswert.

SVV Die Zertifizierung übermittelter Informationen gehört in einem offenen Kommunikationssystem zur notwendigen Infrastruktur, damit die Sicherheit im elektronischen Geschäftsverkehr gewährleistet werden kann. Mit der Zertifizierungsverordnung vom April 2000 wurde in diesem Bereich in der Schweiz ein erstes Mal legiferiert. Wegen der schwachen Kompetenzgrundlage, auf welcher die Verordnung erlassen wurde, ist allerdings bereits damals eine Vorlage auf Gesetzesstufe in Aussicht gestellt worden. Unter Einbezug der Problematik des Verhältnisses der digitalen Signatur zur handschriftlichen Unterschrift löst die Vorlage dieses Versprechen ein.

Im Einklang mit der Gesamtwirtschaft haben wir bereits bei anderen Gelegenheiten auf die Dringlichkeit einer Rahmenordnung für den elektronischen Geschäftsverkehr hingewiesen. Wir begrüssen insofern auch die Teilung des Gesamtprojekts in zwei Vorlagen, denn dadurch dürfte einer schnellen Inkraftsetzung der Regelungen zur Infrastruktur und der Gleichstellung der elektronischen Signatur mit der handschriftlichen Unterschrift, die im Interesse aller Beteiligten liegen, nichts im Wege stehen. Wegen der besonderen Umstände im elektronischen Geschäftsverkehr, namentlich wegen der Gefahr eines Fehlklicks, möchten wir an dieser Stelle aber auch unsere Bereitschaft zum Ausdruck bringen, in die Diskussion zu den Aspekten des Konsumentenschutzes einzutreten, die Gegenstand der zweiten Vorlage bilden. In Anbetracht der unterschiedlichen Positionen der verschiedenen interessierten Kreise, sind weiterführende Diskussionen in diesem Bereich allerdings nicht unwahrscheinlich.

Wie erwähnt, entspricht die Vorlage den Bedürfnissen der Wirtschaft weitgehend. Sie schafft verbesserte Rahmenbedingungen für den E-Commerce. Die Europatauglichkeit, die wegen der Bedeutung des elektronischen Geschäftsverkehrs über die Landesgrenzen hinaus in dieser Vorlage mehr denn je gefragt ist, scheint gegeben zu sein. Da die entsprechenden Richtlinien den einzelnen Gliedstaaten einen erheblichen Regelungsspielraum überlassen, kann diese Frage hier allerdings nicht abschliessend beurteilt werden. Insbesondere in Bezug auf die Haftung wäre eine Koordination mit den Bestimmungen der Gliedstaaten der EU wünschenswert, damit im internationalen Geschäftsverkehr mehr oder weniger einheitliche Regime zur Anwendung gelangen.

Die Vorlage zum BGES stösst in der schweizerischen Versicherungswirtschaft auf breite Unterstützung. Grundsätzlich positiv wird auch der Ansatz taxiert, bezüglich der Gleichstellung der elektronischen Signatur mit der handschriftlichen Unterschrift eine generelle Regelung im OR festzuhalten, ohne alle Einzelgesetze abzuändern, die betroffen sein könnten. Um einzelnen Wirtschaftsbereichen allerdings keine unnötigen Hindernisse in den Weg zu stellen, drängen sich aber dennoch weitere Änderungen auf. Was die Versicherungswirtschaft betrifft, ist namentlich das Versicherungsvertragsrecht anpassungsbedürftig. Entsprechende Anträge haben wir bereits im Rahmen der Teilrevision zum VVG gestellt, soweit Artikel betroffen sind, die dem E-Commerce hinderlich sein können. Da dieser Revisionsprozess zur Zeit noch läuft und sich in einem weiteren Punkt eine Anpassung aufdrängt, erlauben wir uns, diese

versicherungsspezifischen Anliegen auch in die vorliegende Stellungnahme einzubringen (vgl. Ziff. 33).

Bevor wir die Bestimmungen einzeln kommentieren, möchten wir kurz auf einige Punkte hinweisen, die uns im Rahmen der Diskussionen aufgefallen sind. So fehlt in unseren Augen eine Erwähnung des Zeitstempels. Gerade im Vertragsrecht wird dieses Werkzeug oftmals in Kombination mit der elektronischen Signatur zur Anwendung gelangen. Wenn es sich dabei auch grundsätzlich um ein Problem des Obligationenrechts handelt, so würde sich wegen des engen Bezugs der Unterschrift mit dem Zeitpunkt, zu welchem sie gesetzt wurde, eine Begriffsbestimmung im BGES rechtfertigen. Weiter ist zu bemerken, dass die Neutralität der angewendeten Technologie als Leitsatz in das Gesetz aufgenommen werden sollte, damit technische Anforderungen nicht die Entwicklung neuer technologischer Verfahren erschweren, wie dies bspw. durch die grosse Regelungsdichte des deutschen Signaturgesetzes zu befürchten ist.

TSM Die elektronischen Kommunikationsmittel sind aus dem geschäftlichen und privaten Alltag nicht mehr wegzudenken. Wichtig ist, dass die juristischen Grundlagen die wirtschaftliche Entwicklung nicht bremsen, sondern eine sichere und gerechte Basis dafür sind.

Die neuen Erlasse (resp. Teilrevisionen) beinhalten einen guten Ansatz. Sie gehen jedoch für die TSM und sicher auch für andere Unternehmungen zu wenig weit. Insbesondere die Teilrevisionen, welche sich grundsätzlich nur auf privatrechtliche Rechtshandlungen beziehen, sind als Lösung für die TSM unzureichend. Aus unserer Sicht wäre es nötig, die elektronische Signatur in einem neuen und vollständigen Erlass möglichst ganzheitlich zu regeln. Zumindest, soweit die Kompetenzen beim Bund liegen. Die generelle Gleichstellung der elektronischen mit der handschriftlichen Unterschrift bei allen Rechtshandlungen und der strafrechtliche Schutz durch die Tatbestände der Urkundenfälschung und des Betrugs sollte in diesem Erlass ausdrücklich vorgesehen sein.

Eine weitere Anforderung ist die einfache Handhabung der Verschlüsselung und der Entschlüsselung. Einerseits sollte der administrative Aufwand, um in den Besitz eines Schlüssels zu kommen, möglichst gering sein, wobei die Sicherheit der elektronischen Signatur keine Einbussen erleiden darf. Anderseits darf der technische Vorgang der Ver- und Entschlüsselung und die Installation der Software auch für Laien keine grösseren Schwierigkeiten bieten. Zudem sollte der Zeitaufwand für die genannten Vorgänge und die Übertragung des Dokuments an sich nicht wesentlich höher sein, als ohne Verschlüsselung.

VIT Die elektronischen Signaturen stellen eine der wesentlichen Massnahmen zur Förderung des Vertrauens in den E-Commerce dar. Die Mehrheit der Mitglieder des Verbandes Inside Telecom (VIT) unterstützen alle sinnvollen Massnahmen zur Förderung des E-Commerce, da sie einerseits Dienstleistungen für die am E-Commerce beteiligten Unternehmen und Kunden erbringen und andererseits selbst mit Angeboten im E-Commerce auftreten.

Aus Sicht der Mitglieder unseres Verbandes kommt daher der Einführung verbindlicher rechtlicher Rahmenbedingungen für die elektronischen Signaturen eine hohe Priorität zu und die Inkraftsetzung des entsprechenden Gesetzes hat hohe Dringlichkeit. Andererseits darf die Dringlichkeit nicht auf Kosten der Qualität des Gesetzes gehen. Die Ergebnisse des Vernehmlassungsverfahrens sind daher entsprechend zu berücksichtigen.

VSG Nell'ambito delle modifiche che interverranno se dovesse essere accolta la legge federale sulla firma elettronica si prevede l'introduzione del nuovo art. 15a

CO. Questa norma permetterà di concludere anche per via elettronica i contratti che oggi richiedono la forma scritta semplice o per i quali le parti hanno convenuto la forma scritta.
Non vengono toccate dalla novella legislativa i contratti che richiedono la redazione a mano del loro testo (fideiussione, testamento olografo) oppure l'atto pubblico. Questa precisazione è di estrema importanza per le procedure davanti agli Uffici del registro (URF e URC).
Questo nonostante le iscrizioni nel registro fondiario e di commercio, secondo quanto affermato dall'autorità federale, poggiano praticamente sempre su un atto pubblico. Questa posizione non corrisponde alla realtà.
In ogni caso, i principi fondamentali della protezione della verità del contenuto dei registri, della sicurezza nelle procedure davanti all'Ufficio dei registri (URF e URC) e del divieto di trarre in inganno i terzi non possono essere pregiudicati.
Spontanea qualche domanda. Questi principi/interessi sono sufficientemente tutelati in caso di „traffico elettronico“? I dati archiviati a registro fondiario e registro di commercio saranno sufficientemente protetti? Le parti interessate saranno sufficientemente tutelate dal contrarre in modo affrettato?
Potrà essere garantito il mantenimento del contenuto delle dichiarazioni diffuse per via elettronica? Sarà efficace la verifica dell'identità delle parti disponenti? A quale determinato momento si potranno fare risalire gli effetti della nascita dei diritti reali nell'ambio di comunicazioni per E-Mail? Quali ripercussioni ci saranno sulla tenuta dei registri?
Si rileva che la nuova Legge sui fori entrata in vigore in data 1.1.2001 prevede la possibilità di prorogare il foro anche per mezzo di una dichiarazione E-Mail (art. 9).
La preoccupazione principale consiste nel garantire sicurezza a chi usufruisce dei servizi elettronici, in particolare attraverso la creazione di sistemi riconosciuti di certificazione.

VSW Der vollumfänglichen Informatisierung der Dienstleistungen unserer Mitglieder stehen an sich, anders als etwa bei „bricks-and-mortar-companies“ der Warenerzeugung oder des -handels, grundsätzlich keine sachgegebenen Einschränkungen entgegen. Wir befürworten deshalb in besonderem Masse alle legislatorischen Bestrebungen, die darauf abzielen, dem E-Commerce verlässliche rechtliche Grundlagen zu geben und so seine Ausweitung zu fördern. Auch finden wir es richtig, dass der schweizerische Gesetzgeber im Bereich des E-Commerce, der nationale Wirtschaftsräume sprengt, die Regelungen der EU nachvollzieht (RL 1999/93 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen).

312 Negative Gesamtbeurteilung des Vorentwurfs
Appréciation générale négative de l'avant-projet
Giudizio generale negativo sull'avamprogetto

Organisationen / Organisations / Organizzazioni

FGSec Die Arbeitsgruppe PKI der FGSec sieht grundsätzliche technische Voraussetzungen nicht erfüllt, um eine Gleichstellung der Anerkennung elektronischer (digitaler) Signaturen mit handschriftlichen Unterschriften zu erlauben. Insbesondere das Problem der Unterwanderung von Signaturgeräten ist heute nicht gelöst. E-Mail-Clients sind keine und „Sichere Signaturerstellungseinheiten“.

Auch wird die in Teilen fehlende Kompatibilität zur EU-Direktive bemängelt. Es wird Frage gestellt, ob nicht eine weitgehende Kompatibilität angestrebt werden müsste.

Es bestehen weitere Schwächen und Inkonsistenzen, welche uns zur Ablehnung des Vorschlages und zur Forderung einer grundsätzlichen Diskussion und Überarbeitung veranlassen.

SAV Les commentaires qui suivent ont été rédigés dans l'optique de la sécurité du droit pour l'utilisateur non-averti. Il s'agit d'éviter dans la mesure du possible de créer de nouveaux risques juridiques pour les justiciables, risques qui ne seraient pas compensés par des avantages évidents. A l'heure actuelle, chacun est conscient de la fragilité juridique des actes passés par voie électronique. La législation proposée risque de modifier cette impression en la remplaçant par une fausse impression de sécurité, par exemple parce que la distinction entre une signature valable et une signature dépourvue de protection juridique n'est pas suffisamment claire.

Par ailleurs les commentaires formulés à l'occasion de la procédure de consultation relative à l'ordonnance sur les services de certification restent valables, soit notamment la nécessité d'assurer par la loi le respect de règles que le marché ne produit pas spontanément à savoir, en particulier, garantir la sécurité du droit à long terme, protéger les parties les plus faibles et assurer l'équilibre confédéral tout en protégeant les intérêts de la Suisse dans le cadre international.

A l'occasion de la procédure de consultation sur l'OSCert, nous avions souligné que „eine umfassende Regelung der digitalen Signatur auf Gesetzesebene, einschliesslich der Frage der Rechtsverbindlichkeit von digitalen Signaturen ... ist sinnvoll. Die entsprechenden Arbeiten sollten raschmöglichst vorangetrieben werden." Cette remarque reste valable. Il convient cependant de tenir compte des développements qui sont intervenus dans l'intervalle.

Die Zertifizierungsdienste-Verordnung vom 12. April 2000 ist am 1. Mai 2000 in Kraft getreten, doch liegen die technischen Vorschriften erst seit dem 9. Januar 2001 (im Entwurfstadium) vor. Das bedeutet, dass praktische Erfahrungen mit den neuen Normen noch nicht haben gesammelt werden können und Zertifizierungsdienste-Anbieter noch nicht gemäss den Bestimmungen der Verordnung auf dem Markt tätig sind. Eine Beurteilung der technisch ausgerichteten Vorschriften des neuen Entwurfs erweist sich deshalb im jetzigen Zeitpunkt als praktisch ausgeschlossen. Aus diesem Grunde stellt sich die Frage, ob es sachgerecht ist, so kurzfristig die Verordnung durch ein Gesetz zu ersetzen, selbst wenn nicht übersehen werden kann, dass die Anerkennung der elektronischen Signatur einem grossen praktischen Bedürfnis entspricht. En tout cas, les développements, ou l'absence de développements, sur la base de l'OScert devront être pris en compte avant l'adoption définitive de la loi.

In diesem Zusammenhang lässt sich auch die Trennung der Gesetzesvorlagen in ein Bundesgesetz über die elektronische Signatur und ein Bundesgesetz über den elektronischen Geschäftsverkehr hinterfragen. Ein Zusammenhang zwischen den beiden Entwürfen ist offensichtlich gegeben, insbesondere bei den „Konsumentenschutznormen" im Rahmen der elektronischen Signatur. Überschneidungen können sich auch im Bereich der Haftung ergeben. Diese Trennung könnte die Einheitlichkeit der beiden Gesetzesvorlagen gefährden.

Le projet de loi mis en consultation n'offre pas la sécurité juridique indispensable du point de vue de l'utilisateur inexpérimenté. Toutefois et moyennant quel-

ques ajouts importants, il constitue néanmoins une base utile pour atteindre l'objectif souhaité d'une reconnaissance juridique des signatures électroniques.

SWICO Der SWICO begrüsst die Initiative des Bundesrates, die Regelung der digitalen Signatur an die Hand zu nehmen und die Rechtsunsicherheiten, die im elektronischen Geschäftsverkehr existieren, aus dem Weg zu räumen.

Bei den digitalen Signaturen besteht schon seit längerem ein akuter Handlungsbedarf. Sowohl die EU als auch alle Nachbarländer verfügen über gesetzliche Regelungen zur digitalen Signatur. Mit der EU-Richtlinie vom 13.12.1999 wurde eine einheitliche Regelung für den Europäischen Raum vorgegeben, der sich die Schweiz nicht entziehen kann.

Hier setzt deshalb auch die wichtigste Kritik am Entwurf des Bundes an. In der aktuellen Form ist das Gesetz nicht EU-kompatibel und vermag deshalb nicht zu überzeugen. Insbesondere fehlen klare Regeln zur Anerkennung von Signaturen im internationalen Kontext. Neue Gesetze zum elektronischen Geschäftsverkehr müssen indes auf die internationale Situation abgestimmt werden, sonst legiferieren sie an der Praxis vorbei. Es fehlt zudem eine automatische Anerkennung des durch einen EU-Mitgliedstaat anerkannten Anbieters von Zertifizierungsdiensten bzw. der qualifizierten Zertifikate, welche die EU-Richtlinie erfüllen.

Wir halten fest, dass durch dieses Gesetz keinerlei Präjudizien für die Anerkennung von nicht Signaturgesetz-konformen Zertifikaten geschaffen werden soll. Auch in Zukunft wird die Mehrheit der digitalen Signaturen nicht diesem Gesetz entsprechen. Im Rahmen der Parteiautonomie sollen die Benutzer nach wie vor frei sein, die für sie tauglichen Unterschriftssurrogate vertraglich festzulegen bzw. zu akzeptieren. Dieser Grundsatz soll explizit im Gesetz aufgenommen werden.

Der Gesetzesentwurf ist eine Übernahme der Zertifizierungsdiensteverordnung und damit auf eine Technologie fixiert. Ein Signaturgesetz sollte alle möglichen Verfahren beinhalten und keines ausschliessen. Wird ein Verfahren favorisiert, muss dieses aber dann detaillierter geregelt werden. Die im aktuellen Entwurf enthaltenen Delegationen gehen zu weit und lassen einen zu grossen Interpretationsspielraum zu. Selbst die EU-Richtlinie, welche eben „nur" eine Richtlinie ist, ist in vielen Belangen präziser als der Entwurf. So kann eine gesetzliche Haftungsregelung bzw. Risikozuordnung nur dann so festgelegt werden, wenn entsprechend sichere Komponenten zur Verfügung stehen, was im Einzelfall auch erlaubt, die Regelung eindeutig anzuwenden – womit auch die Rechtssicherheit gewährleistet ist.

Zusammenfassend kann festgehalten werden, dass wir es ausserordentlich begrüsst hätten, wenn der Gesetzesentwurf EU-Richtlinie-kompatibel gewesen wäre. Sodann ist u.E. aus Gründen der Rechtssicherheit zwingend vorausgesetzt, dass die Ausführungsbestimmungen gleichzeitig mit dem Gesetz in Kraft treten, namentlich angesichts des hohen Stellenwertes im heutigen Konzept des Gesetzes (technische, qualitative und sicherheitsmässige Anforderungen als Grundlage für den Sorgfaltsmassstab und die Regelung der Risikozuweisung).

Die Haftungsklauseln sind grundsätzlich zu überdenken. Ohne klare Verweise auf die Sorgfaltspflicht der Beteiligten ist die vorgesehene Lösung unklar und lässt vieles offen. Die angestrebte Rechtssicherheit kann man damit nicht erreichen.

Anschliessend möchten wir noch bemerken, dass es für uns nicht verständlich ist, dass für die Erarbeitung des Gesetzesentwurfes keine Expertenkommission

beigezogen wurde, die sowohl internationale Erfahrung als auch Industrie Know-how hätte einbringen können. Damit hätte man den heute berechtigten Vorwurf „Geschwindigkeit statt Qualität“ entkräften können.

1. Mit keinem Wort wird auf die Notwendigkeit der Anpassung an die internationale Entwicklung hingewiesen. Insbesondere fehlen Bezüge zur massgeblich anwendbaren EU-Richtlinie zur digitalen Signatur 1999/93/EG vom 13.12.1999.

2. Dieses Gesetz hat keinen Einfluss auf die Privatautonomie. Den Parteien steht es frei, im geschlossenen, weil privatrechtlich vereinbarten Kontext, Signatursysteme einzusetzen, die nicht diesem Gesetz entsprechen. Dieser Grundsatz sollte explizit festgehalten werden.

3. Das Gesetz trägt (so gut wie die neue OR-Bestimmung Art. 15a) den Begriff „elektronische Signatur“, schränkt jedoch mit der Bestimmung „Geltungsbereich“ dessen Anwendung auf die Technologie „digitale Signatur“ ein. Diesbezüglich beschreitet das BGES im Verhältnis zu andernorts getroffenen Regelungen einen eigenen Weg. Bei einer Fixierung auf eine Technologie fehlen aber die notwendigen Rahmenbedingungen, wie sie z.B. in der EU-Richtlinie in den Anhängen beschrieben sind. Wir schlagen vor, das BGES so zu ergänzen, dass es für alle Formen der Signatur anwendbar sein könnte, ein bestimmtes Verfahren aber bevorzugt und auch genauer beschreibt (vgl. Signaturgesetz Deutschland, SigG, in der verabschiedeten Version vom 15.2.2001).

4. Bei diversen Bestimmungen wird ausgeführt, dass der Bundesrat (BR) die Kompetenz erhält, näheres zu regeln (in den Erläuterungen wird in diesem Zusammenhang vereinzelt auf Art. 23 verwiesen). Es ist zwingend notwendig, dass überall dort, wo der BR die Regelung im Rahmen der Technischen Ausführungsbestimmungen i.S. von Art. 23 BGES zu treffen hat, dies im BGES auch festhält - sei es in der jeweiligen einzelnen Bestimmung, sei es aufzählend in Art. 23.

5. Mindestanforderungen an die digitale Signatur und an das (qualifizierte) Zertifikat in technischer wie qualitativer Hinsicht sind unbedingt notwendig und im Gesetz festzuhalten. Diese Anregung steht im Spannungsfeld zw. Flexibilität der Regelung und Rechtssicherheit. Entsprechend muss bei der Formulierung solcher Mindestanforderungen beachtet werden, dass zwar der Spezifikationsgrad erhöht wird, ohne sich (zu sehr) hinsichtlich der Regelungsmöglichkeiten auf Verordnungsebene einzuengen. Demnach sind im BGES gewisse Mindestanforderungen - vergleichbar zur EU-Richtlinie - an die digitale Signatur bzw. an Kryptographie und privaten Signaturschlüssel sowie an das Zertifikat, sowohl in technischer wie auch in qualitativer Hinsicht, festzuhalten.

6. Mit der Aufnahme der Haftungsbestimmungen sowohl für Inhaber der privaten Signaturschlüssel als auch der Anbieter von Zertifizierungsdiensten müssen die technischen Anforderungen und die Sphärentheorie unmittelbar im Gesetz abgebildet werden. Konkret bedeutet dies:

   - eine klare Abgrenzung der Verantwortlichkeiten
   - eine Beschreibung der Verantwortlichkeiten für die Auswahl der technischen Komponenten
   - eine Beschreibung der Verantwortlichkeiten für kritische Operationen

- Mindestanforderungen an technische Komponenten
- Einsatz von Attributen zum Schutz für den Unterzeichner und die damit verbundene Verpflichtung für die Drittpersonen (Relying Parties), diese zu prüfen
- Klare Ausformulierung der Aufklärungs- und Sorgfaltspflicht.

Es gilt grundsätzlich zu überlegen, ob an dieser Stelle nicht grundsätzlich auf eine Haftungsklausel verzichtet werden sollte.

7. Hinsichtlich der Technischen Ausführungsbestimmungen sollte sichergestellt werden, dass die derzeitigen Aktivitäten sich bereits am BGES orientieren und nicht allein auf die Regelungen in der ZertDV abstellt.
8. Zwecks Lesbarkeit und Steigerung der Verständlichkeit würde es sich u.E. empfehlen, auf jeweilige Beifügung der weiblichen Form des „Inhabers“, des „Kunden“, des … in den Gesetzesbestimmungen zu verzichten.
9. Bei allen nachfolgenden Überlegungen darf nicht ausser Acht gelassen werden, dass die OR-Änderung schwergewichtig im Rahmen der Gleichstellung von „eigenhändiger Unterschrift“ mit „elektronischer Unterschrift“ insbesondere hinsichtlich formbedürftiger Rechtsgeschäfte (mit dem Gültigkeitserfordernis der „einfachen Schriftlichkeit“) steht. Denn elektronisch geschlossene Rechtsgeschäfte mit/ohne elektronischer Signatur gibt es in der Wirtschaft schon seit längerer Zeit. Und, Dokumente/Belege solcher Rechtsgeschäfte unterliegen heute und morgen (also auch nach Inkrafttreten des BGES) der freien richterlichen Beweiswürdigung. In diesem Zusammenhang stellt sich immerhin die Frage, inwiefern die Haftungsbestimmungen im BGES nicht auch für andere elektronische Signaturen und andere elektronische Legitimationsmittel wegweisende Rechtsauswirkungen haben (wo z.B. keine anerkannte Zertifizierungsstelle das Zertifikat ausstellte oder wo nicht das Verfahren der digitalen Signatur eingesetzt wurde) bzw. diese gar analog beigezogen werden oder Umkehrschlüsse daraus gezogen werden.
10. Die automatische Anerkennung von in der EU zugelassenen Zertifizierungsdiensten bzw. von qualifizierten Zertifikaten, die durch diese Dienste ausgestellt wurden, soll im Gesetz aufgenommen werden.

32 Zu den einzelnen Bestimmungen des Vorentwurfs
Des dispositions particulières de l'avant-projet
Le singole disposizioni dell'avamprogetto

321 Bundesgesetz über die digitale Signatur
Loi fédérale sur la signature digitale
Legge federale sulla firma elettronica

321.01 Art. 1

Kantone / Cantons / Cantoni

AR Die elektronische Signatur ist vorderhand ein Institut des privaten Rechtes. Der Amtsverkehr ist davon nicht betroffen. Das Gesetz ist aber für den Verkehr im Steuerwesen insoweit von Interesse, wie es präjudizierend auch für eine Lösung im Verkehr mit Amtsstellen wirkt. Zur generellen Verbreitung der digitalen Signatur ist erforderlich, dass der Bund - wohl in Zusammenarbeit mit internationalen Gremien - benutzerfreundliche Technologien fördert und technische Komponenten zertifizieren hilft. Bereits - etwa im Projekt „guichet virtuel“ - ein-

geleitete Aktivitäten in diese Richtung sind zu verstärken. Wird mit der digitalen Signatur nämlich die handschriftliche Unterschrift bei Vertragsschlüssen ersetzt, bildet dies gleichsam den „oberen Abschluss“ des Einsatzumfelds der digitalen Signatur. Viel häufiger und viel wichtiger wird der Einsatz der digitalen Signatur aber zur Identifikation oder für sicheres E-Mail und zum Abschluss formloser Verträge sein. Hier wird sie - wie bereits erwähnt - zu einem zentralen Instrument des Datenschutzes. Aus Sicht der Kantone ist es daher vordringlicher, dass ihr hier durch die Förderung sicherer Komponenten zum Durchbruch verholfen wird. Der Gesetzesentwurf bietet Gelegenheit, dies in Erinnerung zu rufen.

Da das E-Government wie erwähnt nur am Rande vom BGES betroffen ist, erübrigen sich wohl weitere Ausführungen. Hinzuweisen ist jedoch darauf, dass die Umstellung auf eine elektronische Kommunikation von Bürgern und Behörden die personellen und finanziellen Ressourcen der Kantone beanspruchen wird. Zudem sind allfällige Schwierigkeiten aufgrund der verschiedenen Standards bei den betroffenen Behörden zu beachten. Für die Kantone bedeutet dies, dass sie zur Einführung von E-Government in ihren Erlassen - beispielsweise zur Gültigkeit einer elektronischen Eingabe, aber auch für den elektronischen Informationsaustausch zwischen Behörden und Bürgern - nicht auf die Lösung des BGES zurückverweisen dürfen. Die vom BGES ausgehenden Impulse bestehen daher in erster Linie in der grundsätzlichen Anerkennung der eingesetzten Technologie und - allenfalls in einer späteren Phase - in den durch Bundesrats- oder Departementsverordnungen ausgehenden Technologieregelungen tieferer Stufe.

BE Gemäss dem vorliegenden BGES macht sich kein Zertifizierungsdiensteanbieter strafbar, wenn er Zertifizierungsdienste anbietet, ohne vorgängig um eine Anerkennung nachgesucht zu haben (Begleitbericht zum Entwurf, Stand Januar 2001, Ziff. 210. 011, S. 15). U. E. erscheint es nicht offensichtlich, dass bei dieser Konstellation der vorgesehene Schutz des Konsumenten, welcher in der Pflicht des Anbieters zur korrekten Deklaration der angebotenen Dienstleistung besteht, ausreichend ist. Insbesondere fällt in diesem Zusammenhang auf, dass das Freizeichnungsverbot von Art. 18 BGES nur für anerkannte Anbieter von Zertifizierungsdiensten gilt und in den übrigen Fällen lediglich die Bestimmungen betreffend die Wegbedingung der Haftung gemäss OR und UWG zur Anwendung kommen.

BS Wenn man in diesem Absatz den relativen Nebensatz weglässt, dann lautet der Hauptsatz folgendermassen : „[1]Dieses Gesetz regelt die Voraussetzungen und deren Rechte und Pflichten“. Dieser Satz ist für sich allein nicht verständlich. Wir schlagen Ihnen folgende Fassung vor: „[1]Dieses Gesetz regelt die Rechte und Pflichten anerkannter Anbieterinnen von Zertifizierungsdiensten und die Voraussetzungen, unter denen sie anerkannt werden“.

FR Le projet de loi sous-entend de ce fait que les moyens technologiques déployés afin de mettre en œuvre la signature électronique devraient aboutir à l'introduction de celle-ci. Ainsi, l'art. 1 du projet a pour but de promouvoir la fourniture de services de certification sûrs à un large public. Au niveau de la protection des données, ce but ne met pas uniquement en évidence le fait que la signature électronique sera mise sur pied d'égalité avec la signature manuscrite, mais permet bien plus d'accélérer davantage encore le développement de la technologie y relative. L'application élargie de la cryptographie constitue un moyen essentiel à la protection des données. En effet, grâce aux procédures cryptographiques, les données échangées par voie électronique seront certes con-

traignantes, mais aussi confidentielles, intègres et authentiques. La cryptographie est donc un moyen indispensable tant à la protection des données qu'à leur sécurité.

JU L'objectif formulé à la let. b de l'al. 2 pose problème dans sa formulation, en ce sens que si la loi sur la signature électronique a effectivement pour but de construire un cadre permettant de prévoir l'équivalence des signatures manuscrite et électronique, ce n'est pas elle qui prévoit cette équivalence. Il a à cet égard d'ailleurs été précisé qu'il n'était pas question d'étendre de façon généralisée une telle équivalence dans le projet de loi sur la signature électronique, mais de la limiter au Code des obligations.
Le Gouvernement de la République et Canton du Jura estime dès lors qu'il y a lieu de dissocier clairement les objectifs visés par le projet de loi sur la signature électronique de ceux visés par le projet d'insertion d'un nouvel article 15a dans le Code des obligations.

LU Nicht Inhalt des eigentlichen Gesetzesentwurfs ist die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift. Dies wird erst mit der entsprechenden Ergänzung des Obligationenrechts (neuer Art. 15a) realisiert. Art. 1 Abs. 2 Bst. b Entwurf ist deshalb zu streichen.

GR Aus Sicht des Datenschutzes ist nicht nur die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift von Relevanz, sondern insbesondere die hierbei zugrunde liegende Technologie. Der Einsatz und die Verbreitung der Kryptographie sind dabei wichtige Postulate des Datenschutzes. Dank kryptographischen Verfahren kann für die elektronische Datenkommunikation nicht nur Verbindlichkeit, sondern auch Vertraulichkeit, Integrität und Authentizität gewährleistet werden. Die Kryptographie unterstützt zentrale Anliegen des Datenschutzes und der Datensicherheit. Aus Art. 1 des Gesetzesentwurfs ergibt sich nun der Hinweis, dass die für digitale Signaturen generell vorgesehene Technologie hohen Ansprüchen genügen und damit dem Anliegen des Datenschutzes Rechnung getragen werden soll. Darauf ist bei der praktischen Umsetzung besonders zu achten.

SG Als unbefriedigend erachten wir die fehlende Transparenz, die sich aus dem vorgeschlagenen Grundsatz ergibt, wonach die Anerkennung für Anbieterinnen von Zertifizierungsdiensten freiwillig sein soll. Benutzerinnen und Benutzer könnten sich für den Abschluss eines bestimmten Rechtsgeschäftes vor die Wahl gestellt sehen:

- traditionelle – schon heute praktizierte – Verfahren ohne Zertifikate;
- Verfahren mit „nicht-anerkannten“ elektronischen Zertifikaten;
- Verfahren mit „anerkannten“ elektronischen Zertifikaten.

Damit wäre – insbesondere im Hinblick auf die konkreten Rechtsfolgen der unterschiedlichen Verfahren – die notwendige Transparenz für die Kundschaft nicht gewährleistet, zumal sie in den entsprechenden Angeboten wohl gerade nicht auf die fehlende Anerkennung aufmerksam gemacht würden. Unseres Erachtens wäre es sinnvoller, mit der Anerkennung einer Anbieterin von Zertifizierungsdiensten die Auflage zu verknüpfen, wonach diese ausschliesslich Zertifizierungsdienste anbieten darf, für deren Erbringung sie sich anerkennen liess. Damit könnte vermieden werden, dass eine anerkannte Anbieterin von Zertifizierungsdiensten auch noch Zertifizierungsdienste anbietet, welche die Bundesgesetzgebung über die elektronische Signatur nicht vorsieht.

VD Le projet aurait pu reprendre la dénomination „prestataire de service de certification“ adoptée par la Directive 1999/93/CE du parlement européen et du Conseil.

ZG Das Gesetz hat nicht nur zum Ziel, die elektronische Signatur der eigenhändigen Unterschrift gleichzustellen, sondern auch „ein breites Angebot an sicheren Diensten der elektronischen Zertifizierung zu fördern“ (Art. 1 Abs. 2 Bst. a BGES). Damit wird auch die hier zugrunde liegende Technologie, insbesondere Einsatz und Verbreitung der Kryptographie, gefördert. Verbindlichkeit, Vertraulichkeit, Integrität und Authentizität sind zentrale Anliegen des Datenschutzes und der Datensicherheit. Aus der Sicht des Datenschutzes ist dieses Ziel positiv zu würdigen.

Parteien / Partis / Partiti

Jungfreisinnige Das Signaturgesetz gilt nur für privatrechtliche Verträge. Diese zeichnen sich aber meistens durch Formfreiheit aus. Es gibt also nicht viele zwingende Einsatzgebiete für die digitale Signatur. Natürlich werden viele Verträge im privatrechtlichen Bereich mit einer Unterschrift besiegelt. Dies ist nun auch auf elektronischem Wege möglich. Das Signaturgesetz hat dadurch klar ihre Daseinsberechtigung. Das Gesetz regelt aber weder die notarielle Beglaubigung noch öffentlichrechtliche Belange.
Ein wesentlicher Aspekt fehlt also. Das BGES regelt nicht die elektronische Signatur im Bereich des eGovernments. Die Jungfreisinnigen sehen im eGovernment-Bereich eine grandiose Möglichkeit, die Verwaltungen zu modernisieren und im Rahmen des new public management neu zu organisieren. Der Bundesrat hat in seiner Strategie für eine Informationsgesellschaft in der Schweiz vom 18. Februar 1998 klare Grundsätze gelegt. Auch der 2. Bericht der Koordinationsgruppe Informationsgesellschaft (KIG) an den Bundesrat setzt klar auf das eGovernment. Der Bund betreibt oder plant nicht weniger als 35 eGovernment-Projekte, darunter auch das Prestige Projekt guichet virtuel. Durch den Einbezug der digitalen Signatur im öffentlichrechtlichen Bereich auf Bundesebene kann dieses Projekt nur gewinnen, da dadurch zusätzliche interessante Dienstleistungen für den Bürger generiert werden können. Ein weiteres wichtiges Projekt ist das e-Voting. Auch hierfür wird eine digitale Signatur auf Bundesebene notwendig sein. Auf diese Umstände muss eingegangen werden. In Kapitel 15 des Begleitberichts zum Entwurf verweisen Sie auf die Kompetenzen der Kantone. Der Bund sollte aber in diesem Bereich mit gutem Vorbild vorausgehen und mit der Integration des eGovernment in das BGES eine Signalwirkung für die Kantone bewirken. Wir möchten noch auf einen Kommentar von David Rosenthal in der NZZ vom 9. März 2001 verweisen. Er spricht über das eGovernment und meint es sei vor allem wichtig, garantieren zu können, dass die Daten während der Übermittlung nicht abgeändert werden. Nachdem nun das Signaturgesetz eine solche Garantie ermöglichen würde, würde es Sinn machen „die neuen Bestimmungen über den elektronischen Behördenverkehr nötigenfalls in den Schnellzug der BGES-Vorlage umzuladen, denn diese dürfte auf weniger Widerstand stossen als die Justizreform.
Erweiterung des Einsatzgebietes der digitalen Signatur auch auf die öffentlichrechtliche Ebene. Dabei sollen die eGovernment-Projekte des Bundes als Signal für die Kantone gelten.

Organisationen / Organisations / Organizzazioni

Briner Das Gesetz regelt deutlich mehr, als was in Art. 1 Abs. 1 gesagt wird. Es regelt insbesondere auch Rechte und Pflichten der Privaten.

EKK La Directive européenne 1999/93/CE sur un cadre communautaire pour les signatures électroniques opère une distinction entre, d’une part, les dispositifs de création de signature et les dispositifs sécurisés de création de signature et,

d'autre part, entre le certificat et le certificat qualifié. Le projet susmentionné n'a pas repris ces distinctions. Or, selon l'art. 5 de la Directive précitée, seules les signatures électroniques basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier.

La Commission demande que le Conseil fédéral étudie ce problème pour garantir au consommateur que seules les signatures électroniques basées sur un certificat qualifié et créées par des dispositifs sécurisés soient assimilées à la signature manuscrite.

Elle demande aussi que la LFSél prévoie un système d'horodatage (Zeitstempel) qualifié avec une certification qualifiée portée sur la signature électronique d'un fournisseur de services de certification selon laquelle des données électroniques lui ont été fournies à un certain moment donné. Ceci pour faciliter notamment la preuve du moment où le document a été transmis.

FGSec Es ist bisher nicht klar, ob BGES-Unterschriften auf den High-End-Teil des Marktes abzielen – wo hohe Kosten vertretbar sind und die Zertifikate eher punktuell verwendet werden würden – oder ob sie den mittleren Bereich abdecken sollen, in welchem eine erschwingliche Lösung für einen grossen Marktanteil sorgen würde. Das BGES und der Begleitbericht implizieren hier unterschiedliche Zielsetzungen: Das BGES ignoriert das Problem der sicheren Signaturerstellungseinheit, und der Begleitbericht impliziert, dass ein E-Mail-Client für diesen Zweck akzeptabel ist.

Zu Abs. 1: Das Gesetz regelt auch die Verwendung der elektronischen Signatur, der Haftung der Nutzer und Zertifizierdienststellen (CSPs) usw.

Zu Abs. 2 Bst. b: „Gleichstellung" ist irreführend, denn es bestehen wesentliche Unterschiede. Im Besonderen hat die Beweislastumkehr zwar gleiche Rechte, aber viel mehr Pflichten zur Folge. Nur die Anerkennung ist gleichgestellt, nicht die Unterschrift.

FSP En page 30, le rapport explicatif précise que „ le présent projet de loi fédérale sur la signature électronique correspond aux dispositions du droit européen. Concernant la levée des exigences de forme constituant un obstacle à la conclusion des contrats par la vole électronique, il va même plus loin que ce qui est exigé par le droit européen. Le projet ne fait pas usage de toutes les possibilités d'exclure la conclusion d'un contrat par la vole électronique auxquelles un Etat membre peut recourir „

Même si notre Fédération a toujours souhaité une législation nationale „eurocompatible", elle estime indispensable, compte tenu des dérives que peut entraîner une mauvaise utilisation de la signature électronique, d'élaborer en la matière une réglementation très claire et susceptible de prévenir tous les abus.

Notre Fédération retient que, munie d'une signature électronique, toute déclaration de volonté pour laquelle une signature manuscrite était jusqu'alors exigée, pourra être valablement transmise (par voie électronique) si le destinataire de la déclaration a la possibilité de la recevoir. Nous ignorons cependant ce que cela signifie concrètement.

Cette question se pose avec d'autant plus d'acuité que la liste des actes juridiques pouvant valablement être formés par la voie électronique n'est pas clairement définie. A cet égard, il serait judicieux d'anticiper pour éviter de devoir attendre que des questions fondamentales soient réglées par la jurisprudence.

Il suffit pour nous en convaincre de lire le rapport explicatif. Ce rapport fait état d'un bon nombre de questions pratiques sans nous éclairer sur la façon de les résoudre.
Il ressort ainsi de celui-ci que certaines signatures - notamment numériques - seront reconnues et protégées par la loi. Cela soulève certaines d'interrogations, parmi lesquelles :

- Quel sera le nombre des signatures ainsi reconnues ?
- Quelle en sera la nature ?
- Quelle(s) relation(s) pourra-t-il y avoir avec les signatures non reconnues par la loi ?
- Quelles informations envisage-t-on de communiquer aux personnes susceptibles de conclure des contrats par la voie électronique ?

Face à ce flou pratique et juridique, notre Fédération se demande comment l'utilisateur pourra y voir clair, et quelles en seront les conséquences.

KVN Die Aussage im Begleitbericht „Kein Zertifizierungsdienstanbieter macht sich strafbar, wenn er Zertifizierungsdienst anbietet, ohne vorgängig um eine Anerkennung nachgesucht zu haben ....“ darf auf keinen Fall so angewendet werden, da diese im Widerspruch zu Art. 1 Abs. 1 steht.

Muster/Sury Es wäre sinnvoll, von der Systematik her eine genaue Unterscheidung, möglichst in folgender Reihenfolge, betreffend folgender Fragen zu erreichen:

1. Aufsicht betreffend Rechtsverhältnis zwischen Zertifizierungs- und Anerkennungsstelle.
2. Regelung des Verhältnisses zwischen Zertifizierungsstelle und Zertifikatsbezüger (-nutzniesser), (z.B. die Pflicht, die AGB zu publizieren und dem Kunden vor Vertragsabschluss auszuhändigen).
3. Regelung der Haftung im Umgang mit digitalen Zertifikaten unter den Zertifikatsbezügern (-nutzniesser) selber. Dies sollte in das Obligationenrecht einfliessen.
4. Rechte und Pflichten des Staates im Umgang mit digitaler Signatur. Dies sollte in den entsprechenden Verordnungen der Registerführung einfliessen.

Beim Gesetzesentwurf steht vor allem der Vertragsabschluss mittels elektronischer Signatur im Zentrum. Denn es geht vor allem um das Bedürfnis, Dokumente elektronisch zu signieren und so Verträge über das Telekommunikationsnetz abschliessen zu können. Dabei wird ausser Acht gelassen, dass auch ein Bedürfnis besteht, mittels digitaler Zertifikate und dem dazu passenden privaten Schlüssel vertrauliche Nachrichten zu versenden. Mittels der asymmetrischen Kryptographie und der digitalen Zertifikate besteht die Möglichkeit, vertrauliche Mitteilungen auszutauschen.
KMUs und die zur Vertraulichkeit verpflichteten Personen (Anwälte, Ärzte, Priester und deren Hilfspersonen) sollten die ihnen anvertrauten Berufsgeheimnisse in vertraulicher Form austauschen können. Mittels der anerkannten Zertifizierungsstellen versprechen sie sich unter Umständen, so eine günstige Teillösung zur vertraulichen Kommunikation untereinander zu finden. (Teillösung deshalb, weil noch die Sicherheitssoftware für die Verschlüsselung beschafft werden muss.)
Dieses Bedürfnis könnte möglicherweise indirekt durch das vorliegende Gesetz auch abgedeckt werden, es müsste aber mit Sicherheit überprüft werden können, wem Zertifikate zugeordnet werden.

SAV Trois éléments sont essentiels pour assurer la sécurité juridique en matière d'utilisation des signatures électroniques, si l'on se place du point de vue de l'utilisateur non expérimenté : une validité juridique générale, une distinction claire entre les signatures électroniques juridiquement valables et celles qui ne le sont pas, et la possibilité de déterminer exactement quand la signature électronique a été utilisée.
Les documents munis d'une signature électronique au sens de la LFSél doivent être valables en Suisse comme des documents écrits munis d'une signature manuscrite. Il est impossible de demander aux utilisateurs de consulter à chaque fois la législation fédérale ou cantonale applicable pour savoir si dans un cas la transmission est juridiquement valable ou si elle ne l'est pas, ou si elle ne l'est qu'à condition de respecter des conditions de forme supplémentaires. Seule l'adoption d'un principe clair et général offre la sécurité juridique nécessaire.

SBB Die rechtliche Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift wird im neuen Art. 15a OR geregelt. Das BGES, welches in seinem Anhang die Einführung dieser neuen Bestimmung vorschlägt, hat nur indirekt zum Zweck, diese Gleichstellung zu regeln, sondern sie will lediglich die technischen Voraussetzungen dieser Gleichstellung festlegen. Bst. b ist vor diesem Hintergrund besser in Abs. 1 von Art. 1 zu integrieren.

SBV La définition de l'„objet" de la loi pourrait être complétée comme suit:
„La présente loi définit *les conditions de l'équivalence entre les signatures électroniques et les signatures manuscrites ainsi que les droits et les devoirs des fournisseurs de services de certification et des détenteurs de certificats.*"
„Dieses Gesetz regelt *die Voraussetzungen, unter denen elektronische Signaturen mit der eigenhändigen Unterschrift gleichgestellt sind,* und *die* Rechte und Pflichten *von Anbieterinnen von Zertifizierungsdiensten und Inhabern von Zertifikaten*".

SICTA Im neuen Bundesgesetz wird die elektronische Signatur, welche von einem anerkannten Zertifizierungsanbieter stammt, der eigenhändigen Unterschrift gleichgestellt. Wir erachten es als richtig, dass die Anpassung mit einer Änderung des Obligationenrechts vorgenommen wird, ohne alle Einzelgesetze, die von den Formvorschriften betroffen sind, einzeln abzuändern. Wir gehen davon aus, dass auch all diese Anpassungen mit der heutigen Vorlage abgedeckt sind. Wichtig erscheint uns insbesondere, dass die elektronische Unterschrift das Kriterium „Schriftform" in allen Rechtsgebieten erfüllt. Der vorliegende Gesetzesentwurf lässt zwar manche Fragen der Praxis unbeantwortet, doch ist das Gesetz hiermit gegenüber der Rechtsentwicklungen offener. Gerade die technischen Aspekte in der Vorlage werden den Entwicklungen angepasst werden müssen. In diesem Zusammenhang stellen wir fest, dass die Kompetenz des Bundesrates für den Erlass von Ausführungsbestimmungen inkl. möglicher Subdelegation sehr weit geht. Diesem Vorgehen, welches aus der stark technischen Natur der Vorlage begründet wird, ist grundsätzlich nur zuzustimmen, wenn auch zu den vorgesehenen Ausführungsbestimmungen wiederum die betroffenen Kreise und die Wirtschaftsorganisationen angehört werden.

SWICO Gesetzestitel und Zweckartikel stimmen nicht überein. Der Zweck muss sein, die Rahmenbedingungen für elektronische Signaturen (hier als Oberbegriff für alle Formen der elektronischen Unterschrift) zu schaffen. Die Umschreibung des Gegenstandes muss vervollständigt werden, so etwa durch Einfügung des kursiv gesetzten Textteils: „Dieses Gesetz regelt *die Voraussetzungen, unter*

denen elektronische Signaturen mit der eigenhändigen Unterschrift gleichgestellt sind, und die Rechte und Pflichten von Anbieterinnen von Zertifizierungsdiensten und Inhabern von Zertifikaten.“

321.02 Art. 2

Kantone / Cantons / Cantoni

GE Le principe de la neutralité technologique est essentiel, car il répond au souci du législateur de codifier des schémas juridiques susceptibles de survivre à l'évolution fulgurante des techniques. Son respect implique la recherche de critères de distinction objectifs, ne dépendant pas de la technique spécifique employée. Cet aspect est particulièrement important en matière de sécurisation des transmissions en ligne et, notamment, de signature électronique où les progrès techniques sont constants.

Les codifications existantes, en particulier la directive communautaire du 13 décembre 1999, ainsi que le projet de loi uniforme de la Commission des Nations Unies pour le droit commercial international (CNUDCI), insistent d'ailleurs sur le respect de ce principe. La procédure de consultation menée par l'Office fédéral de la communication (OFCOM) avant l'adoption de l'ordonnance sur les services de certification électronique, du 12 avril 2000 (OSCert) a également relevé l'importance de ce même principe. Il n'a pourtant pas été consacré dans le cadre de l'ordonnance elle-même, au motif que d'autres textes réglementaires pourraient être édictés le moment venu. Or, si cet argument était acceptable dans le cadre d'une ordonnance, dont l'adoption ou la modification peuvent être relativement rapides, il ne l'est plus pour une loi fédérale.

En effet, de deux choses l'une : soit le projet adopte la conception et la structure d'une loi cadre, comme l'est la directive communautaire du 13 décembre 1999, et le respect du principe de la neutralité technologique doit impérativement être suivi, soit le projet de loi fédérale sur la signature électronique se consacre exclusivement à un système de signature électronique fondé sur une cryptographie asymétrique (infrastructure à clé publique), mais la réglementation en matière de signature électronique est alors incomplète.

Il ressort du rapport explicatif accompagnant le projet que le Conseil fédéral avait l'intention de respecter le principe de la neutralité technologique. Or, il faut malheureusement constater que la formulation actuelle de la loi n'atteint pas ce but.

L'art. 2, al. 2 et 3 du projet prévoit certes une délégation en faveur du Conseil fédéral qui peut étendre le champ d'application de cette future loi à d'autres formes de signature électronique en arrêtant les dispositions d'exécution „dans la limite des principes dégagés par la (présente) loi“. Or, cette délégation de compétence ne pourra vraisemblablement pas être mise en œuvre sans violer le principe constitutionnel de la séparation des pouvoirs. A cet égard, la délégation ne peut intervenir que dans un cadre clairement défini par le législateur. Or, la référence générale aux „principes dégagés par la présente loi“, paraît trop vaste pour éviter le risque d'une délégation abusive. Certes, selon le rapport explicatif, ces principes concernent toutes les techniques susceptibles de s'assurer de l'intégrité des données transmises et de les authentifier. Néanmoins, tous les articles du projet, sans exception, n'ont de sens que dans le cadre d'une infrastructure à clé publique et ne peuvent être étendus à d'autres techniques. Ainsi, sous une formulation prétendument neutre, c'est bien un système basé sur une infrastructure à clé publique, et lui seul, qui est réglementé par le législateur.

La question se pose en des termes encore plus aigus pour ce qui est de l'assimilation, dans certaines situations, de la signature électronique à la signature manuscrite. A cet égard, la formulation du nouvel art. 15a du code des obligations est particulièrement symptomatique et viole clairement le principe de la neutralité technologique. Il dispose en effet : „lorsqu'un contrat est conclu par un échange de données électroniques, la signature électronique est assimilée à la signature manuscrite au sens de l'art. 14, lorsqu'elle repose sur un certificat d'un fournisseur de services de certification reconnu au sens de la loi fédérale sur la signature électronique". Ainsi, tout mécanisme d'authentification autre que la cryptographie asymétrique est exclu. C'est dire que des systèmes comme l'examen des empreintes digitales ou de la rétine, par exemple, ne seraient pas considérés comme étant suffisamment sûrs pour que cette assimilation soit reconnue.

Il paraît donc essentiel de modifier, sur ce point déjà, le projet d'art. 15a du code des obligations en faisant, par exemple, référence à „tout procédé de signature électronique réglementé par la loi fédérale sur la signature électronique".

NE La délégation de compétence en faveur du Conseil fédéral en ce qui concerne la reconnaissance d'autres formes de signature électronique que la signature numérique est adéquate.

Elle permet une extension du champ d'application correspondant au développement technique de plus en plus rapide des moyens informatiques tout en respectant les principes de sécurité garantissant l'authenticité et l'intégrité des documents électroniques.

TI Si tratta di disposizioni generiche, che per essere applicate richiedono norme esecutive tecniche particolareggiate. L'evoluzione rapidissima che si riscontra in questo settore imporrà frequenti adeguamenti della legislazione alle novità tecnologiche ed è quindi necessario che la legge deleghi le modalità di esecuzione a normative che possono essere modificate in breve tempo.

VD S'il est heureux de constater que le Conseil fédéral peut étendre le champ d'application de la loi à d'autres formes de signature électronique, l'on peut se demander si l'extension sera compatible avec l'art. 15a nouveau du Code des obligations. Nous reviendrons sur cette question ci-après lorsque nous commenterons ledit article.

JU Au niveau formel, le renvoi à l'art. 3, let. b, de même que celui à l'article 3, lettre a, ne sont pas nécessaires. Par ailleurs, les al. 2 et 3 forment un tout par rapport à l'al. 1, ce qui ne résulte pas immédiatement de la structure actuelle de cette disposition.

Pour le reste, il paraît effectivement souhaitable de pouvoir étendre le champ d'application de la loi au gré des développements techniques. Il convient cependant de relever que le présent projet de loi est élaboré au regard d'un mode particulier de signature électronique et qu'il n'est pas aisé de déterminer si une extension du champ d'application pourra se réaliser sans que cela ne nécessite une adaptation ultérieure de la loi.

<u>Organisationen / Organisations / Organizzazioni</u>

Briner Das Gesetz soll Bundesgesetz über die *elektronische* Signatur heissen, aber in Art. 2 Abs. 1 wird gesagt, es gelte nur für die *digitale* Signatur. Damit werden alle Regelungen, die sich auf elektronische Signaturen beziehen, in gewisser Weise vorab entwertet. Art. 2 sollte so formuliert werden, dass klar die „elektronische" Signatur geregelt wird; sachgerecht ist, dass vorderhand nur die im

Entwurf als „digital“ bezeichnete Signatur besonders geregelt und mit besonderen Rechtswirkungen ausgestattet wird. Wir verweisen auch auf unsere Bemerkungen gleich nachfolgend zu Art. 3 des Entwurfs.

Clusis Wie / Comme / Come GE.

CP Le champ d'application ne s'étend qu'à la signature numérique, le Conseil fédéral restant compétent de l'élargir en cas de nouveau développement technologique. Cela nous semble tout à fait judicieux.

FGSec Die aktuellen Ausführungsbestimmungen (Entwurf) beziehen sich auf die Zertifizierungsdiensteverordnung, und nicht auf das BGES.

FRI Le système mis en place nous semble extrêmement complexe. Le montage proposé, qui met en scène les fournisseurs de services de certification reconnus (art. 2) ou non reconnus, les organismes de reconnaissance et l'organisme d'accréditation, mérite selon nous une simplification.

Notre proposition consiste à supprimer la distinction entre organisme de reconnaissance et organisme d'accréditation, comme le suggère le libellé de l'art. 5 al. 2 du projet.

Jeune Barreau vaudois Im selben Sinne wie / Dans le même sens que / Nello stesso senso di GE.

SAV Die Unterscheidung zwischen elektronischer und digitaler Signatur (Art. 3 lit. a und b) überzeugt nicht vollumfänglich. „digital“ (en français: „numérique“) ist der Gegensatz zu „analog“ und bezeichnet die Art und Weise, wie moderne Computersysteme rechnen; „elektronisch“ ist ein mit Elektrizität arbeitendes Gerät. Abgesehen davon, dass die Signatur selber nicht elektronisch sein kann, ist es auch möglich, eine digitale Signatur auf Papier auszudrucken und hernach zur Überprüfung wieder in einen Computer einzulesen. Das sprachlich exakte Gegenstück zum „Prüfschlüssel“ ist nicht der „Signaturschlüssel“, sondern der „Signierschlüssel“.

Ce problème de terminologie recouvre en fait la difficulté qui résulte de la volonté d’élaborer une loi sur la reconnaissance des signatures électroniques qui soit neutre du point de vue de la technologie utilisée, mais qui en fait repose quand même exclusivement sur l’utilisation de certificats électroniques.

Face à la nécessité d’assurer une certaine stabilité au niveau de la loi mais face également à la rapidité de l’évolution technologique et à la nécessité d’une coordination internationale on est amené à prévoir des délégations de compétence très (dans certains cas trop) larges. Cette façon de faire implique au moins que les dispositions d’exécution soient connues au moment où la loi est débattue.

Les codifications existantes, en particulier la directive communautaire du 13 décembre 1999, ainsi que le projet de loi uniforme de la Commission des Nations Unies pour le droit commercial international (CNUDCI), insistent d'ailleurs sur le respect du principe de la neutralité technologique. La procédure de consultation menée par l'Office fédéral de la communication (OFCOM) avant l'adoption de l'ordonnance du 12 avril 2000, a également relevé l'importance de ce même principe. Il n'a pourtant pas été consacré dans le cadre de l'ordonnance elle-même, au motif en particulier que d'autres textes réglementaires pourraient être édictés le moment venu. Si cet argument était acceptable dans le cadre d'une ordonnance dont l'adoption ou la modification peut être relativement rapide, il ne l'est plus pour une loi fédérale.

De deux choses l'une : soit le Projet adopte la conception et la structure d'une loi cadre, comme c'est le cas de la directive communautaire du 13 décembre 1999, et le respect du principe de la neutralité technologique doit être impérati-

vement suivi, soit le projet de loi fédérale sur la signature électronique se consacre exclusivement à un système de signature électronique fondé sur une cryptographie asymétrique (infrastructure à clé publique), mais la réglementation en matière de signature électronique est alors incomplète.

En l'espèce, il ressort du rapport explicatif accompagnant le Projet que le Conseil fédéral avait l'intention de respecter le principe de la neutralité technologique. Or, il faut malheureusement constater que la formulation actuelle de l'article 2 du projet n'atteint pas ce but. Il ressort en effet de cette disposition que la délégation de compétences en faveur du Conseil fédéral, *„habilité à arrêter des dispositions d'exécution dans la limite des principes dégagés par la présente loi“* ne pourra vraisemblablement pas être mise en œuvre sans violer le principe constitutionnel de la séparation des pouvoirs. A cet égard, il importe de rappeler que toute norme d'application générale qui serait édictée par le pouvoir exécutif doit reposer soit sur une base légale, soit sur une base constitutionnelle suffisante. Par ailleurs, la délégation ne peut intervenir que dans un cadre défini par le législateur ou le constituant. En l'espèce, la référence générale aux *„principes dégagés par la présente loi“*, paraît trop vague pour éviter le risque d'une délégation abusive. Certes, selon le rapport explicatif, ces principes concernent toutes les techniques susceptibles de s'assurer de l'intégrité des données transmises et de les authentifier (ch. 210.012). Néanmoins, tous les articles du Projet, sans exception, n'ont de sens que dans le cadre d'une infrastructure à clé publique et ne peuvent être étendus à d'autres techniques. Ainsi, sous une formulation prétendument neutre, c'est bien un système basé sur une infrastructure à clé publique, et lui seul, qui est réglementé par le législateur.

SBV L'art. 2 du projet de loi habilite le Conseil fédéral à étendre le champ d'application de la loi en fonction des développements techniques ultérieurs. Cette délégation de compétences répond certes à un besoin de flexibilité. Force est néanmoins de constater que l'approche techniquement neutre du projet, qui se traduit à l'article 2 alinéa 2, ne paraît guère cohérente avec le reste de la loi. Le projet de loi traite en effet pour l'essentiel de l'émission de certificats numériques qualifiés au sein d'une infrastructure à clé publique. Quant aux „principes dégagés par la présente loi“, sur lesquels le Conseil fédéral doit se fonder pour arrêter les dispositions d'exécution concernant d'autres formes de signatures électroniques (cf. alinéa 3), nous ignorons à quelles dispositions de la loi les auteurs du projet entendent se référer. Cette question devrait être clarifiée dans l'ordonnance.

La législation proposée n'a pas d'incidence sur la liberté contractuelle des parties. Celles-ci conservent la faculté de convenir de l'utilisation de certificats électroniques ne remplissant pas les exigences de la loi. Il serait important que cette clarification soit apportée dans la loi.

SIK Zu diesem Punkt möchten wir festhalten, dass der Text *praktisch* andere Algorithmen als das erwähnte Public-Key-Verfahren ausschliesst (trotz entspr. Hinweisen auf gleichwertige Verfahren), was bedenklich ist. Gewiss glauben wir auch, dass es unwahrscheinlich ist, dass sich andere, ebenbürtige Verfahren in der nächsten Zukunft durchzusetzen vermögen. Eine Anpassung des Textes, um diese technische Abhängigkeit zu eliminieren, wäre u.E. zu aufwendig und deswegen sehen wir ein, dass sie sich kaum aufdrängt.

SWICO Erfasst wird die Regelung der „Elektronischen Unterschrift“ mit dem Verfahren der digitalen Signatur als derzeit einzig möglicher Lösung.

Schlauri/Kohlas Art. 2 des Vorentwurfs differenziert zwischen elektronischen und digitalen Signaturen: Mit der „elektronischen Signatur“ wird ein allgemeiner

Oberbegriff für Signaturverfahren eingeführt. Der Begriff der digitalen Signatur hingegen soll für Signaturverfahren stehen, die auf einer Public-Key-Infrastruktur basieren – es handelt sich also um einen Unterbegriff zur elektronischen Signatur.
Ziel dieser Unterteilung ist die „technologieneutrale“ Ausgestaltung des Erlasses: Es soll vermieden werden, durch eine vorschnelle Fixierung auf bestimmte Verfahren (d.h. Verfahren mit Public-Key-Infrastruktur) die technische Entwicklung zu hemmen.
Die immer wieder zu hörende Forderung nach Technologieneutralität scheint auf der Annahme zu basieren, dass eine ganze Reihe verschiedener möglicher Konzepte zur Realisierung digitaler Signaturen denkbar seien. Dem ist jedoch, zumindest was die Grundprinzipien der Verfahren anbelangt, nicht so: Jedes Verfahren zur Sicherung von Integrität und Authentizität digitaler Kommunikation ohne Möglichkeit zu sicheren (d.h. nichtdigitalen) Erstkontakten zwischen den Kommunikationsteilnehmern muss in irgendeiner Form auf einem beglaubigten öffentlichen und einem zu diesem korrelierenden geheimen Parameter basieren: Wenn der öffentliche Parameter (bzw. dessen Beglaubigung) fehlt, kann eine Überprüfung nicht stattfinden, ohne den geheimen Parameter preiszugeben, und wenn der geheime Parameter fehlt (d.h. der öffentliche zum Signieren eingesetzt wird), ist jedermann in der Lage, eine Signatur zu setzen. Dies gilt genauso für die gelegentlich als Beispiele für elektronische Signaturen ins Feld geführten biometrischen Systeme: Die Biometrie dient regelmässig nur dazu, den geheimen Parameter vor unbefugtem Zugriff zu schützen. Rein biometrische Systeme können ausschliesslich zu Authentifizierungszwecken (etwa zur Eingangskontrolle), nicht jedoch zur Sicherung der Dokumentenintegrität eingesetzt werden.
Die Vorstellung, dass in Zukunft auch elektronische Unterschriften ohne eine zugrundeliegende Public-Key-Infrastruktur Einsatz finden könnten, ist damit u.E. unrealistisch. Es gibt keine „elektronischen Signaturen“ im Sinne des Vorentwurfs, die nicht gleichzeitig auch „digitale Signaturen“ wären. Eine Unterscheidung zwischen elektronischer und digitaler Signatur erübrigt sich, und es sollte ausschliesslich der Begriff der „digitalen Signatur“ eingesetzt werden.
Der Einsatz der Ausdrücke „elektronisch“ und „digital“ zur Differenzierung zwischen Signaturverfahren ist zudem aus sprachlichen Gründen abzulehnen: Der Ausdruck „digital“ steht im Gegensatz zu „analog“, bedeutet „in Stufen erfolgend“ oder „schrittweise“ und bezeichnet damit die Art und Weise, wie moderne Computersysteme rechnen. „Elektronisch“ ist ein mit Elektrizität arbeitendes, aus Halbleitern oder dergleichen aufgebautes Gerät. „Elektronische Daten“ und damit auch „elektronische Signaturen“ gibt es in diesem Sinne streng genommen gar nicht. Die Ausdrücke „digital“ und „elektronisch“ sind damit zur Unterscheidung von Signaturverfahren ungeeignet und für den Nichteingeweihten verwirrend.
Auch die Tatsache, dass insbesondere der Begriff „elektronische Signatur“ im internationalen Umfeld (etwa in der EU-Signaturrichtlinie oder im bundesdeutschen Gesetz über Rahmenbedingungen über elektronische Signaturen) bereits eingesetzt wird, sollte nicht dazu verleiten, dessen Einsatz nicht noch einmal kritisch zu überdenken.

321.03 Art. 3

Kantone / Cantons / Cantoni

AG Aus Sicht des Datenschutzes ist zu prüfen, dass auch die Benutzung von Zertifikaten unter einem Pseudonym ermöglicht wird. Dies wird durch den BGES-Entwurf jedoch explizit ausgeschlossen. Bei der Pseudonymisierung geht es - entgegen den Ausführungen im erläuternden Begleitbericht (S. 16) - nicht (primär) um die Wahrung der Vertraulichkeit bei der Übermittlung, sondern darum, dass eine unter Pseudonym auftretende Person - anhand eines Zertifikats - zweifelsfrei als dieselbe Person identifiziert werden kann (s. dazu: Bizer, Datenschutz und Datensicherheit / DuD, 1 / 1997 S. 46, Gateway). Es ist darauf hinzuweisen, dass das deutsche Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz / SigG) in § 7 Abs. 1 Ziff. 1 die Möglichkeit des Pseudonyms ausdrücklich zulässt.

BL Wie / Comme / Come AG.
Vgl. auch zu Art. 8 / Cf. également ad art. 8 / Cfr. anche ad art. 8.

FR Contrairement à ce que stipule la LFSél, la protection des données exige que l'utilisation d'un pseudonyme doit être rendue possible lors de l'emploi d'un certificat. En effet, l'utilisation d'un pseudonyme n'est pas prioritairement destinée à augmenter la confidentialité de la personne qui l'utilise, tel que le suppose le rapport explicatif (p. 16), mais de lui permettre d'être reconnue par un système comme étant la même personne (cf. à Ce sujet Bizer, DuD 1/97, p. 46; Gateway).

GE De nombreuses critiques se sont déjà élevées en ce qui concerne l'absence d'obligation, pour les fournisseurs de services de certification, de délivrer des services de „time stamping“. Il faut en effet rappeler que la durée de validité d'un certificat électronique est limitée et peut être révoquée en tout temps. Ainsi, pour que la signature électronique reposant sur un certificat valable puisse être assimilée à une signature manuscrite au sens du projet d'art. 15a nouveau du code des obligations, il s'agirait nécessairement d'exiger qu'elle soit accompagnée d'un tampon temporel pouvant attester du moment auquel la signature est intervenue. En l'absence d'une telle indication, le signataire pourrait en effet prétendre que la signature est intervenue ultérieurement à la révocation du certificat.

GL Wie / Comme / Come AG.

JU Le Gouvernement de la République et Canton du Jura se rallie à l'option consistant à n'attribuer les certificats électroniques qu'à des personnes physiques, mais non à des personnes morales, ces dernières agissant de toute manière par l'intermédiaire d'une ou de plusieurs personnes physiques. De même, il paraît exclu qu'une personne physique puisse se voir attribuer un certificat sous le couvert de l'anonymat du pseudonyme.

SG Wir beantragen, Art. 3 Bst. c wie folgt zu formulieren: „*privater Signaturschlüssel*: geheim gehaltene und einmalige *elektronische* kryptografische Schlüssel, die zur Erstellung einer digitalen Signatur verwendet werden;“
Begründung: Zwischen Art. 3 Bst. c und d besteht eine terminologische Differenz, die zu Auslegungsschwierigkeiten führen könnte.
Wir beantragen, Art. 3 Bst. g wie folgt zu formulieren: „*Anbieterin von Zertifizierungsdiensten*: *Stelle, die elektronische Zertifikate ausstellt;*“
Begründung: Der Begriff der elektronischen Umgebung ist ungenau und entbehrlich; der Begriff der Beglaubigung sollte nur in Bestimmungen über die öffentliche Beurkundung verwendet werden.

Wir beantragen, in Art. 3 einen neuen Bst. h mit folgendem Wortlaut einzufügen: „*Anerkennungsstelle: Stelle, die nach dem Akkreditierungsrecht für die Anerkennung der Anbieterinnen von Zertifizierungsdiensten zuständig ist.*“
Begründung: Die nötigen Begriffsumschreibungen sind in Art. 3 zusammenzufassen. Die zusätzliche Definition entspricht inhaltlich Art. 5 Abs. 1 Satz 1.
Wir beantragen, auf die im Begleitbericht zu Art. 3 Bst. f angedeutete Zulassung von Zertifikaten, die auf Pseudonyme lauten, zu verzichten. Die Bezeigung der Person, auf die das Zertifikat lautet, muss amtlich korrekt sein.

VD A la let. a de cette disposition, le projet ne distingue pas la „signature électronique“ de la „signature électronique avancée“, au contraire de la directive européenne susmentionnée. Le projet implique ainsi que la „signature électronique“ permet à la fois le contrôle de l'intégrité des données et leur authentification.
A la let. b, la formulation suivante serait plus claire : „(…) *d'une clé privée qui peut être vérifiée* (…)“.
A propos de la let. f, la page 15 du rapport explicatif mentionne que les certificats électroniques basés sur le projet de loi ne peuvent être attribués qu'à des personnes physiques au motif qu'un certificat attribué à une personne morale donnerait une fausse impression que cette personne dispose de la possibilité de s'engager directement alors que le droit actuel ne le permet pas. Même si les problèmes juridiques motivant cette option sont compréhensibles, l'on peut regretter les difficultés pratiques qu'elle engendrerait pour les autorités cantonales qui souhaiteraient obtenir un certificat électronique.
Toujours à ce propos, l'on peut se demander ce qui se passera si le certificat est délivré à une personne physique déterminée en sa qualité d'organe d'une personne morale, en cas de changement d'organe. Notons que l'art. 2, ch. 5 du projet de loi belge du 15 février 2001 prévoit expressément que la délivrance d'un certificat électronique à une personne morale est possible.
Enfin, l'on peut se demander dans quelle mesure l'usage de la signature électronique n'implique pas également l'apposition infalsifiable d'une datation du document signé.
Le projet de loi ne prévoit pas l'utilisation d'un pseudonyme. Cela risque d'entraver la reconnaissance de certificats délivrés par des fournisseurs étrangers dont la réglementation autorise l'utilisation d'un pseudonyme.

ZG Art. 3 listet die Begriffe auf, die das Gesetz verwendet. Uns fehlen jedoch im Gesetz die Definitionen der Begriffe „Identifizierung“ und „Authentizität“ bzw. „Authentifizierung“. Insbesondere der Begriff „Identifizierung“ im Sinne des Gesetzes geht über den normalen Sprachgebrauch hinaus. Darunter wird auch die Unveränderbarkeit der elektronischen Meldung verstanden. Dies müsste im Gesetz aufgezeigt werden.
Bei der Verwendung von elektronischen Zertifikaten sollte gemäss Art. 3 Bst. a BGES insbesondere die Integrität der Daten sichergestellt werden. Dabei kann es nur um die Richtigkeit von Rohdaten - also um eine korrekte Abfolge von Bits - gehen. Dies genügt jedoch nicht, da sich eine Vielzahl von Präsentationsproblemen stellen können, die ihren Grund in der Konfiguration der verwendeten Datenbearbeitungsanlage beim Daten-Empfänger haben (vgl. dazu Ulrich Pordesch, in DuD 2 / 2000 S. 89 ff.). Die Probleme rund um die Präsentation sind unseres Erachtens im Gesetz explizit zu lösen.
Auch wäre es zu begrüssen, wenn das Erfordernis eines Zeitstempels explizit im Gesetz erwähnt würde.
Aus Sicht des Datenschutzes ist zu prüfen, dass auch die Benutzung von Zertifikaten unter einem Pseudonym ermöglicht wird. Dies wird durch den BGES-

Entwurf jedoch explizit ausgeschlossen. Bei der Pseudonymisierung geht es - entgegen den Ausführungen im erläuternden Begleitbericht (S. 16) - nicht (primär) um die Wahrung der Vertraulichkeit bei der Übermittlung, sondern darum, dass eine unter Pseudonym auftretende Person - anhand eines Zertifikats - zweifelsfrei als dieselbe Person identifiziert werden kann (s. dazu: Bizer, Datenschutz und Datensicherheit / DuD, 1 / 1997 S. 46, Gateway). Es ist darauf hinzuweisen, dass das deutsche Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz / SigG) in § 7 Abs. 1 Ziff. 1 die Möglichkeit des Pseudonyms ausdrücklich zulässt.

Parteien / Partis / Partiti

PLS Il ne sera pas toujours aisé de prouver qu'un certificat électronique était valide au moment exact où les partenaires contractuels ont conclu une transaction donnée. Pour supprimer toute incertitude à ce sujet, il serait judicieux de prévoir un système d'horodation („time stamping„).

Organisationen / Organisations / Organizzazioni

Briner Es ist sicher richtig, die „elektronische Signatur" als Oberbegriff zu verwenden, wie das auch die europäische Richtlinie 1999/93/EG tut. Es ist ebenso richtig, im Gesetz grundsätzlich alle elektronischen Signaturen zu erfassen, aber vorläufig nur die heute bekannte Signatur mit dem Public/Private-Key mit besonderen Rechtswirkungen auszustatten.

Die begriffliche Erfassung dieser Situation scheint uns aber verbesserungsbedürftig. Sie ist zunächst rein gesetzestechnisch recht verwirrlich. Man veranschaulicht das wohl am besten mit Art. 3 lit. f des Entwurfes, gemäss welchem ein „elektronisches" Zertifikat eine Bescheinigung bezüglich einer „digitalen" Signatur ist, die gemäss Art. 3 lit. b mit Hilfe eines „privaten" Signaturschlüssels erstellt wird, der gemäss Art. 3 lit. c ein „kryptographischer" Schüssel ist. Das sind der Begriffe zuviel. Ein weiteres Beispiel ist Art. 7 des Entwurfs.

Sodann ist der begriffliche Unterschied zwischen „elektronisch" und „digital" verschwommen, weil in Art. 3 lit. b die „digitale" Signatur als eine „elektronische" Signatur bezeichnet wird, die als Public/Private-Key-System funktioniert. Das Wort „digital" wird in einem unnötig einengenden Sinne verwendet. Es kann sehr wohl noch andere „digitale" Signatursysteme als kryptographische mit Public/Private-Key geben.

Die Formulierung „im Rahmen einer elektronischen Umgebung" (Art. 3 lit. g) ist nicht nur Fachjargon, sondern unpräzise und unklar. Wir wüssten jedenfalls nicht, wie die Formulierung in korrektes Alltagsdeutsch zu übertragen wäre, weil wir nicht verstehen, was damit ausgedrückt werden soll.

DSB Wie / Comme / Come AG.

FHZ Hier ist ev. zu präzisieren, was genau authentifiziert wird, der Benutzer oder die Daten.

ISACA Les services du fournisseur se limitent à certifier un ensemble de caractères et de signes (des données) et non le sens de ces signes pour le lecteur (l'information). Il serait donc souhaitable de remplacer à la let. g le mot „information„ par le terme „signature électronique„

FGSec Die Terminologie des BGES (Begriffe in Art. 3) muss durch diejenige aus der EU-Direktive ersetzt werden. Dies hat eine Überarbeitung des gesamten Dokuments zu Folge.

Im Besonderen müssen die Begriffe „Qualifiziertes Zertifikat" (Qualified Certificate), „Fortgeschrittene elektronische Signatur" (Advanced Electronic Signature)" und „Sichere Signaturerstellungseinheit" (Secure signature creation de-

vice) verwendet werden. Ausserdem etabliert sich der Begriff „Qualified Certificate" weltweit [RFC 3039] und nicht nur in Europa.
Es bestehen keine Referenzen der Beziehungen zu den EU-Begriffen „Fortgeschrittene elektronische Signatur (Advanced Electronic Signature)", „Qualifiziertes Zertifikat (Qualified Certificate)", und „Sichere Signaturerstellungseinheit (Secure Signature Creation Device)" etc. Vgl. EU-Direktive Art. 2.
Das „Sichere Signaturerstellungseinheit" wird nicht erwähnt. Dies hat ernsthafte Konsequenzen.
Zu Bst. a und b: Der Begriff „digitale Signatur" ist hier neu, stellt das zentrale Element dar, wird aber später nicht mehr verwendet! Der Begriff „elektronische Signatur" stellt zwar notwendige, aber nicht hinreichende Voraussetzungen zur Verfügung. Der Titel „BGES" müsste eigentlich „BGDS" lauten. Die fortgeschrittene elektronische Signatur wird nicht genannt.
Zu Bst. f: Das Zertifikat bindet den Schlüssel an den eindeutigen Namen (Distinguished Name) einer natürlichen Person, nicht an die Person selbst.
Zu Bst. g: Das BGES behandelt nur die Beglaubigung von öffentlichen Schlüsseln, und nicht allgemein die „Daten-Beglaubigung".

Jeune Barreau vaudois Vgl. zu Art. 2 / Cf. ad art. 2 / Cfr. ad art. 2.

Rosenthal Die Begriffsdefinitionen des Art. 3 sind offen und unverbindlich abgefasst. Insbesondere geht aus den Definitionen nicht hervor, welche rechtliche Bedeutung einer elektronischen Signatur bzw. einem „lektronischen" Zetifikat (richtiger- und konsequenterweise müsste in Art. 3 Bst. f von einem *digitalen* Zertifikat gesprochen werden, da es durch den Bezug zum "öffentlichen Schlüssel" ins engere Umfeld der digitalen und nicht elektronischen Signatur gehört) zukommen soll. Diese Unverbindlichkeit wird bewusst so gewählt worden sein, um einzelnen Bestimmungen wie etwa dem vorgeschlagenen Art. 15a OR nicht vorzugreifen. Das ist auch sinnvoll so, da das BGES letztlich eine Basis und Referenznorm für die rechtliche Anerkennung der Signatur in verschiedensten Erlassen des Schweizer Rechts sein soll (und nicht nur im OR).
Da jedoch Art. 15a OR-VE ebenfalls keine explizite Definition des rechtlichen Bedeutungsgehalts einer Signatur liefert, bleiben letztlich auch die Rechtswirkungen des Einsatzes einer Signatur ungeklärt. Die Verfasser des BGES-VE gehen in ihren Erläuterungen stillschweigend davon aus, dass der Einsatz einer Signatur deren Inhaber (Gemeint ist die einer Signatur mittels Zertifikat zugeordnete natürliche Person) verbindlich verpflichten kann, auch wenn er die Signatur nicht selbst erzeugt hat. Dies soll richtigerweise auch so sein, wie noch zu erläutern ist.
Eine klare Regelung einer solchen Rechtswirkung fehlt jedoch weiterhin (Nicht betroffen sind die Fälle, in denen der Inhaber der Signatur diese selbst leistet; er wird dadurch verpflichtet, dass er eine Willenserklärung abgibt (was über die Beweisbarkeit nichts sagt). Aus Sicht der Bindungswirkung kritisch sind nur die Fälle, in denen eine andere Person dies für ihn tut bzw. der Inhaber der Signatur behauptet, er habe sie nicht benutzt. Der BGES-VE sieht keine einzige Bestimmung vor, die der digitalen Signatur eine Rechtswirkung verleiht, die über die Fähigkeit hinaus geht, im Rahmen eines Schriftformerfordernisses nach Art. 12 OR die in Art. 13 OR verlangte Unterschrift zu ersetzen. Auch die Verfasser des BGES-VE gehen offenbar davon aus, dass Art. 15a OR-VE sich auf die Gleichstellung der Signatur alleine zum Zweck der Schriftformerfüllung bezieht. Die restlichen Wirkungen sollen sich implizit ergeben. Das aber sorgt für Unsicherheiten bzw. gibt den Rechtsanwendern einen nach Ansicht des Verfassers zu weiten Spielraum.

Somit bleibt die zentrale Frage unbeantwortet, welchen Bedeutungsgehalt der Empfänger einer Willenserklärung mit ihr beigefügten, (nach BGES) anerkannten Signatur beimessen kann. Es gibt verschiedene Antworten:
a) Nach den knappen (und auch nicht verbindlichen) Äusserungen der Verfasser des BGES-VE zu dieser Frage (Erläuterungen BGES-VE, Nr. 210.072) bedeutet das Vorliegen einer Signatur, dass der tatsächliche (aber nicht notwendigerweise legitimierte) Erzeuger der Signatur damit einzig aussagt, dass er im Namen des Inhabers der Signatur handle, sei es, dass er selbst dieser ist (was unproblematisch ist), sei es, dass er als sein Stellvertreter in dessen Namen auftritt.
b) Nach dem Wortlaut des Art. 3 bedeutet das Vorliegen einer Signatur wiederum nur, dass zwischen dem Inhaber der Signatur und der signierten Willenserklärung irgend ein Zusammenhang besteht, nicht aber welcher. Das OR liefert keine weiteren Erkenntnisse.
c) Der Verfasser dieser Stellungnahme vertritt schliesslich die Ansicht, dass ein digitales Zertifikat die Bekanntgabe einer besonders ausgestalteten Bevollmächtigung gegenüber Dritten darstellt. Demnach sollen zum Abschluss von Verträgen im Namen der im Zertifikat genannten Person all jene ermächtigt sein, die eine gemäss Zertifikat gültige Signatur erzeugen können. Diese Bekanntgabe dieser Bevollmächtigung erfolgt durch den Vertretenen, nicht den Stellvertreter, auch wenn das Zertifikat im Einzelfall durch den Stellvertreter (als Boten) übergeben wird. Die Übergabe des privaten Signaturschlüssels des Signatur-Inhabers (als Vertretener) an den Signierer (als Vertreter) wiederum ist mit der (internen) Erteilung einer Vollmacht vergleichbar. Wird der private Signaturschlüssel entwendet oder kommt er dem Inhaber auf andere Weise abhanden, ist zwar keine (interne) Vollmacht erteilt, die Bevollmächtigung („externe Vollmacht“) müsste aber in der Regel trotzdem als den Vertragspartnern mitgeteilt gelten.
Varianten a) und b) sind praxisfern und bieten nicht die nötige Rechtssicherheit, die sich die Verkehrskreise von der Anerkennung der Signatur richtigerweise erhoffen. Sollte entgegen der Ansicht des Verfassers dieser Stellungnahme trotzdem Variante a) weiterverfolgt werden, so sollte dies wenigstens ausdrücklich festgehalten sein. Die Frage des Bedeutungsgehalts einer Signatur bzw. eines Zertifikats für das Vertragsrecht ist zu wichtig, um übergangen zu werden. Der einzige Anhaltspunkt ist gegenwärtig Art. 17 Abs. 1 BGES-VE, der jedoch seinerseits nur vermuten lässt, dass eine Signatur bzw. ein Zertifikat etwas mit einem Stellvertretungsverhältnis zu tun hat. Eine genauere Erklärung liefern erst die Erläuterungen, die zwar einen gewissen präjudiziellen Charakter haben, letztlich aber nicht verbindlich sind.
Es wäre freilich zu prüfen, ob der Haupttext des BGES tatsächlich eine geeignete Stelle für eine solche Regelung ist, da sie primär das Vertragsrecht betrifft. Auch Art. 17 Abs. 1 BGES-VE passt an sich nicht in das BGES, sondern gehört ins Stellvertretungsrecht des OR (mit „Haftung“ hat Abs. 1 ohnehin nichts zu tun, wie die Marginalie des Art. 17 BGES-VE suggeriert).
Der Verfasser dieser Stellungnahme plädiert an dieser Stelle jedoch dafür, den rechtlichen Bedeutungsgehalt einer Signatur im Rahmen des Stellvertretungsrechts des OR im Sinne von Variante c) explizit festzuhalten. Denn die Verfasser des BGES-VE verkennen nach der hier vertretenen Ansicht, dass die von ihnen ohne nähere Begründung abgelehnte Variante c) (Erläuterungen BGES-VE, Nr. 210.072 [Art. 17]) auch die herrschende Ansicht der am elektronischen Geschäftsverkehr beteiligten Personen ist: Die Mehrheit des angesprochenen

Publikums geht unzweifelhaft davon aus, dass eine Signatur den Inhaber normalerweise verbindlich verpflichtet, gleichgültig, ob diese von einer befugten oder unbefugten Person verwendet wird (Genauso wird kein Bankkunde annehmen, dass er für Geldbezüge von seinem Konto nicht wenigstens teilweise aufkommen müsste, wenn er seine Geldautomatenkarte mit seinem Geheimcode einem Dritten zugänglich macht). Entsprechend ist bereits auch die Kritik etwa aus Kreisen der Konsumentenschützer ausgefallen (Vgl. Vernehmlassungseingabe der Stiftung für Konsumentenschutz vom 29. März 2001 zu Art. 17 Abs. 1 BGES-VE).

Wird der Bedeutungsgehalt einer Signatur nicht wie hier empfohlen ausdrücklich festgehalten, wird der Bedeutungsgehalt einer Signatur (wie andere Willenserklärungen) nach dem Vertrauensprinzip ermittelt werden müssen, was zwar eine gewisse Rechtsunsicherheit schafft, nach Ansicht des Verfassers dieser Stellungnahme letztlich aber ebenfalls zur Annahme von Variante c) führen wird. Art. 17 Abs. 1 BGES-VE würde weitgehend wirkungslos, da Art. 33 Abs. 3 OR bzw. Art. 34 Abs. 3 OR zur Anwendung käme und es auf den Willen des Signatur-Inhabers nicht mehr ankommen würde, ganz gleich, was er beweisen kann. Der Wille des Signatur-Inhabers wäre nur noch dann relevant, wenn der Empfänger der Signatur bösgläubig gewesen wäre, d.h. gewusst hätte (oder wissen musste), dass der Signierer nicht gehörig bevollmächtigt war.

Schlauri/Kohlas Um das Funktionieren einer Public-Key-Infrastruktur zu gewährleisten, ist auch eine Zeitstempel-Infrastruktur notwendig. Daher hier der Vorschlag für einen Artikel, der eine Pflicht der Zertifizierungsdiensteanbieter zur Bereitstellung von Zeitstempeldiensten vorsieht (angelehnt an die Formulierung des deutschen Signaturgesetzes von 1997). Der Artikel wäre wohl vor Art. 13 VE-BGES einzufügen: [1]Die Anbieter von Zertifizierungsdiensten haben digitale Daten auf Verlangen mit einem Zeitstempel zu versehen. [2]Die Artikel 4 und 8 Abs. 2 dieses Gesetzes gelten entsprechend.

Ferner der Vorschlag für einen Art. 3 Bst. h BGES: *„h. Zeitstempel: Bescheinigung dafür, dass bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorlagen.“*

Die in Art. 3 Bst. a VE-BGES verlangte elektronische Form ist ferner für eine digitale Signatur nicht begriffsnotwendig. Eine digitale Signatur könnte mühelos auf Papier ausgedruckt und danach zur Überprüfung wieder in einen Computer eingelesen werden. Sie verliert dadurch ihre Eigenschaft als digitale Signatur nicht.

Damit ist folgende Neuformulierung vorzuschlagen: *„a. digitale Signatur: Daten, die anderen Daten beigefügt oder logisch mit diesen verknüpft sind, um deren Authentizität und Integrität nachzuweisen, und die mit Hilfe eines Signierschlüssels erstellt wurden und mit Hilfe des entsprechenden Prüfschlüssels überprüft werden können.“*

Damit ergibt sich auch der Vorschlag für eine Umbenennung des Gesetzes in ein „Bundesgesetz über digitale Signaturen“.

Das sprachlich exakte Gegenstück zum „Prüfschlüssel“ ist nicht der „Signaturschlüssel“, sondern der „Signierschlüssel“. Der Begriff „Signierschlüssel“ ist zudem eindeutig dem Signiervorgang zugeordnet, während sich „Signaturschlüssel“ auf die Signatur (d.h. das Datenpaket) als solche bezieht und damit im Prinzip auch den Überprüfungsakt betreffen könnte.

Die Definitionen des „privaten Signaturschlüssels“ als „geheim gehaltener kryptographischer Schlüssel“ und des „öffentlichen Prüfschlüssels“ als „allge-

mein zugänglicher kryptographischer Schlüssel“ sind pleonastisch. Die Begriffe „privat“ bzw. „öffentlich“ können auf der linken Seite ersatzlos gestrichen werden.
Überdies ist das in Art. 3 Bst. c genannte Begriffselement der Einmaligkeit beim Signierschlüssel fehl am Platze: Sofern eine Signatur auch ohne Zuhilfenahme einer Hardwaresigniereinheit (Chipkarte o.ä.) gesetzt werden können soll, muss der Signierschlüssel auf Diskette oder Festplatte gespeichert werden. Er ist damit kopierbar und nicht mehr einmalig.
Ferner verwenden die Definitionen der Bst. c und d wohl versehentlich den Plural, während der zu definierende Begriff jeweils im Singular steht, und die Definition des Begriffs „Prüfschlüssel“ wird überflüssigerweise mit dem Begriffselement „elektronisch“ versehen, während dies beim Signierschlüssel unterbleibt.
Damit ergibt sich der folgende Vorschlag:

b. Signierschlüssel: geheimer kryptographischer Schlüssel zur Erstellung digitaler Signaturen.

c. Prüfschlüssel: öffentlicher kryptographischer Schlüssel zur Überprüfung digitaler Signaturen.

Die Zusätze „geheim“ sowie „öffentlich“ zu den Begriffen Signier- resp. Prüfschlüssel können im gesamten Gesetzestext unterbleiben, was elegantere Formulierungen ermöglicht.
Elektronisches Zertifikat: Entsprechend den früher gemachten Ausführungen kann es sich in Art. 3 Bst. f VE-BGES nicht um ein „elektronisches“, sondern nur um ein „digitales“ Zertifikat handeln. Das Gleiche gilt für weitere Vorkommen des Begriffs „elektronisch“ in Bezug auf Daten, wie etwa in Art. 21 VE-BGES.
Die Tatsache, dass eine Anbieterin digitale Zertifikate ausstellt, lässt den Schluss auf die „elektronische Umgebung“ bereits zu. Das Begriffselement kann damit ersatzlos entfallen.
Der Begriff der „Daten“ ist zu weit gefasst: Dabei handelt es sich nur um die Zuordnung von Prüfschlüsseln zu natürlichen Personen. Dies wiederum ist bereits in der Definition des digitalen Zertifikates enthalten und kann damit entfallen.
Es ist schliesslich nicht einzusehen, weshalb durchgehend von Anbieterinnen von Zertifizierungsdiensten gesprochen wird. Dies erstens, weil auch natürliche Personen anerkannt werden können (die in der Gesetzgebung des Bundes bisher durchgehend in der männlichen Form, allenfalls durch die weibliche Form ergänzt, bezeichnet werden), und zweitens, weil der Begriff auch in der männlichen Form schlicht zu unförmig ist, als dass er eine zusätzliche Verlängerung noch ertragen könnte. Der Unterschied im Genus zwischen Definiendum und Definiens (Anbieter / Stelle) ist als kleineres Übel hinzunehmen.
U.E. wäre der Begriff „Zertifizierungsdiensteanbieter“ zudem – trotz seiner Länge – dem Begriff „Anbieter von Zertifizierungsdiensten“ vorzuziehen. Dies deshalb, weil er sich durch ZDA abkürzen lässt und zudem elegantere Formulierungen erlaubt (vgl. etwa den folgenden Titel: „Anerkennung von Anbietern von Zertifizierungsdiensten“ vs. „Anerkennung von Zertifizierungsdiensteanbietern“).
Die Definition kann damit folgendermassen vereinfacht werden: f. [Anbieter von Zertifizierungsdiensten][Zertifizierungsdiensteanbieter]: Stelle, die digitale Zertifikate ausstellt.

Ferner ist zu bemerken, dass für Anbieter von Zertifizierungsdiensten im Vorentwurf durchgehend der Plural verwendet wird, was etwa im Falle von Art. 18 VE-BGES zur Regelung von Art. 97 OR im Gegensatz steht.
Art. 3 Bst. a VE-BGES unterscheidet zwischen Integrität und Authentizität von Texten. Eine solche Unterscheidung ist jedoch logisch streng genommen nicht korrekt: Denn wenn ein Text als nicht authentisch gilt, hat die Prüfung der Integrität keinen Sinn, und wenn ein Text nicht integer ist, ist er gleichzeitig auch nicht mehr authentisch. Authentizität impliziert damit also Integrität, und Integrität impliziert Authentizität. Obwohl diese Unterscheidung teilweise noch heute auch unter anerkannten Kryptologen verwendet wird, sollte sie u.E. unterbleiben.
Im Weiteren ist der Begriff des Inhabers kryptografischer Schlüssel streng genommen nicht korrekt. Es ist grundsätzlich möglich (wenn auch unerwünscht), dass ein Schlüssel mehreren Personen zur Verfügung steht (etwa wenn ein Passwort ausgespäht oder weitergegeben wurde). Diesfalls gibt es keinen alleinigen „Inhaber“ des Schlüssels mehr. Bezeichnet werden sollen im Gesetz regelmässig nicht diejenigen Personen, welche die tatsächliche Kontrolle über einen Schlüssel ausüben (also die „Inhaber“), sondern es ist vielmehr die Person gemeint, zu der im Zertifikat der Schlüssel als zugehörig gekennzeichnet wird.
Es stellt sich die Frage, welcher Begriff diese Zuordnung korrekt ausdrücken könnte. Bis dato konnten wir keine befriedigende Formulierung finden, welche diesen Umstand korrekt ausdrückt. Zur Disposition standen die Begriffe des „Zertifizierten“ (wobei dies insofern unpassend ist, als nicht die Person, sondern die Zuordnung von Schlüssel und Person zertifiziert wird) oder des Zertifikatssubjekts (dieser Begriff ist jedoch nicht aus sich heraus verständlich). Auf einen konkreten Vorschlag für einen Begriff wird daher an dieser Stelle verzichtet.
Anders als das deutsche Signaturgesetz (sowohl in alter als auch in neuer Fassung) sieht der VE-BGES keine Möglichkeit vor, digitale Zertifikate auf ein Pseudonym auszustellen. Der Begleitbericht des Entwurfs begründet dies mit sich daraus ergebenden juristischen Schwierigkeiten und der Möglichkeit, etwa datenschutzrechtlichen Bedenken bereits durch Verschlüsselung gerecht werden zu können, wodurch Pseudonyme unnötig würden (Begleitbericht, 210.013).
U.E. ist die Möglichkeit zur Ausstellung von Zertifikaten auf Pseudonyme aus Gründen des Datenschutzes aber weiterhin prinzipiell wünschenswert. Dies insbesondere deswegen, weil ein Zertifikat bedeutend einfacher Rückschlüsse auf eine Person zulässt als die heute üblichen Techniken des Sammelns von Surferdaten, und weil sich derartige Datensammlungen durch das vom Begleitbericht genannte Verschlüsseln der Übermittlungsstrecke *gerade nicht* vermeiden lassen, da sie regelmässig *durch den Betreiber der besuchten Website selbst erstellt werden*.
Auch ausserhalb des elektronischen Geschäftsverkehrs ist es grundsätzlich möglich, mit Pseudonym oder unter fremdem Namen aufzutreten. Art. 32 Abs. 2 OR kann diesfalls analog zur Anwendung kommen, und der Vertrag ist gültig, wenn es dem Vertragspartner auf die Identität des unter Pseudonym Auftretenden nicht ankommt. Solange aus dem Zertifikat selbst ersichtlich ist, dass es sich beim angegebenen Namen um ein Pseudonym handelt, kann dies dem auf das Zertifikat Vertrauenden in jedem Fall entgegengehalten werden.
Auch die übrigen aus dem Einsatz von Pseudonymen erwachsenden Fragestellungen erscheinen u.E. mittels der bestehenden Gesetzgebung zu Obliga-

tionenrecht, Datenschutz, Berufsgeheimnissen, Geldwäscherei etc. grundsätzlich als lösbar.
Die Verbreitung von auf Pseudonym ausgestellten Zertifikaten könnten zudem gefördert werden, indem die Bestimmbarkeit des richtigen Namens für den Streitfall gewährleistet würde: Eine Aufhebung der Anonymität könnte beispielsweise im Sinne der Aufhebung von Berufsgeheimnissen durch den Richter geschehen. Eine entsprechende Regelung wäre wünschenswert.
Auch die übrigen aus dem Einsatz von Pseudonymen erwachsenden Fragestellungen erscheinen u.E. mittels der bestehenden Gesetzgebung zu Obligationenrecht, Datenschutz, Berufsgeheimnissen, Geldwäscherei etc. grundsätzlich als lösbar.
Die Verbreitung von auf Pseudonym ausgestellten Zertifikaten könnten zudem gefördert werden, indem die Bestimmbarkeit des richtigen Namens für den Streitfall gewährleistet würde: Eine Aufhebung der Anonymität könnte beispielsweise im Sinne der Aufhebung von Berufsgeheimnissen durch den Richter geschehen. Eine entsprechende Regelung wäre wünschenswert.

SBV Art. 3 lit. a: Nous proposons de remplacer, dans cette disposition, „ou“ par „et“.
Art. 3 lit. d: Nous proposons de supprimer, dans cette disposition, le mot „électronique“.
Le texte du projet de loi étant axé sur la cryptographie à clé publique, nous proposons, le cas échéant, de remplacer le terme „certificat électronique“ par „certificat numérique“. Cette remarque vaut pour l'ensemble de la loi.
Identification du détenteur de clés (art. 3 lit. g): L'identification d'une personne demandant l'obtention d'un certificat électronique est une tâche essentielle du fournisseur de services de certification. Nous proposons dès lors de le stipuler clairement, à l'article 3 lettre g du projet de loi, qui pourrait être complété comme suit:
„(…) qui certifie *et atteste l'attribution d'une clé publique à une personne déterminée, clairement identifiée* (…)“.
„(…) die *die Zuteilung eines öffentlichen Schlüssels zuhanden einer bestimmten, eindeutig identifizierten Person beglaubigt und* (…)“.
Horodatation (art. 3 lit. h): Des difficultés peuvent surgir lorsqu'il s'agit d'apporter la preuve qu'un certificat électronique était valide au moment où les parties ont conclu une transaction donnée. Un service d'horodatation („time stamping“) serait de nature à lever cette incertitude. L'horodatation permet en effet de garantir que les signatures numériques ne perdent pas leur validité après l'écoulement de la durée de validité du certificat, respectivement, de sa date de révocation. Nous proposons dès lors de compléter comme suit l'article 3: *„Horodatation: Une attestation numérique munie de la signature numérique d'un fournisseur de services de certification confirmant que certaines données numériques lui ont été présentées à un moment donné.“*
„Zeitstempel: Eine mit einer digitalen Signatur versehene digitale Bescheinigung einer Anbieterin von Zertifizierungsdiensten, dass ihr bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben.“
Cette définition correspond, pour l'essentiel, à celle donnée par la loi allemande révisée sur la signature électronique. Nous vous renvoyons à ce sujet au § 2 chiffre 14 de cette loi („qualifizierte Zeitstempel“).

SIK Zu Bst. a und b: Die Begriffe „elektronische Signatur“ und „digitale Signatur“ sind Begriffe, die in der Praxis kaum auseinanderzuhalten sind. Deswegen erscheint der hier gemachte Unterschied als sehr künstlich und wird vom Publikum kaum verstanden. Offensichtlich geht es bei der hier definierten „digita-

len Signatur“ um eine auf das Verfahren „Public Key“ basierende, digitale Signatur, in anderen Worten um eine „zertifizierte digitale Signatur“. Wir empfehlen, die Begriffe „elektronische Signatur“ und „digitale Signatur“ als äquivalent zu definieren und das Wort „zertifiziert“ überall im Text hinzuzufügen, wo es erforderlich ist, auch wenn der Text damit schwerer wird.

Zu Bst. c und d: Schönheitsfehler: Das Betreff wird im Singular und die Definition im Plural formuliert (sollte nicht nur von uns bemerkt worden sein).

SVV Lit. g. „Anbieterin von Zertifizierungsdiensten: *eine Stelle oder eine juristische oder natürliche Person, die Zertifikate ausstellt oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellt.*“

Eventualantrag: „Anbieterin von Zertifizierungsdiensten: Stelle, die *für eine* elektronische Umgebung Daten beglaubigt und zu diesem Zweck elektronische Zertifikate ausstellt.

Begründung: Nach Vorentwurf hat die Anbieterin von Zertifizierungsdiensten eine Stelle zu sein, die im Rahmen einer elektronischen Umgebung Daten beglaubigt und zu diesem Zweck elektronische Zertifikate ausstellt. Diese Formulierung steht im Widerspruch zu Art. 9, wo für die Beglaubigung die persönliche Vorweisung bestimmter Dokumente verlangt wird; denn die Wendung „im Rahmen“ lässt nämlich in irreführender Weise darauf schliessen, dass die Beglaubigung selbst elektronisch erfolgen könnte. Abgesehen davon, dass diese Möglichkeit theoretisch besteht (vgl. Art. 9 Abs. 2), wird die Beglaubigung in der überwiegenden Mehrheit der Fälle die physische Präsenz des Ansprechers verlangen. Bei der Variante des Hauptantrags handelt es sich um den Text der EU-Richtlinie zur digitalen Signatur. In Anbetracht des Umstandes, dass die Richtlinie selbst eine Definition des Zertifizierungsdiensteanbieters enthält, wäre eine wörtliche Übernahme der Bestimmung angebracht. Da elektronische Signaturen künftig über die nationalen Grenzen hinaus einsatzfähig sein sollten, spielt die Kompatibilität der Vorlage mit der gesetzlichen Situation im Ausland eine entscheidende Rolle. Im Übrigen liesse sich der bereits angesprochene Zeitstempel unter die „anderweitigen Dienste“ subsumieren.

Der Eventualantrag hält sich demgegenüber an den Vorschlag des Vorentwurfs. Wir schlagen darin eine Wendung vor, die Klarheit schafft und gleichzeitig offen genug formuliert ist.

SWICO Art. 3 lit. a: Die Kontrolle der Integrität ist nicht Funktionalität einer „Elektronischen Signatur“. Die Integritätsprüfung ist nur im Falle der digitalen Signatur möglich.

Statt „oder“ sollte es u.E. „und“ heissen.

Art. 3 lit. d: „elektronische“ sollte gestrichen werden bzw. ist überflüssig.

Art. 3 lit. f: Der Begriff „elektronisches Zertifikat“ ist sachlich falsch. Es müsste „Digitales Zertifikat“ heissen. Zudem muss ergänzt werden, dass dieses Zertifikat den im Gesetz noch zu formulierenden Anforderungen genügen muss.

Art. 3 lit. g: Kann man auf die Aktivität des Ausstellens von Zertifikaten beschränken.

Damit digitale Signaturen über das Gültigkeitsdatum bzw. das Revozierungsdatum des zugehörigen Zertifikates hinaus gültig bleiben, müssen sie vorher, d.h. namentlich bei ihrer Erstellung, mit einem digitalen Zeitstempel versehen werden. Ohne Zeitstempel ist eine längere Aufbewahrung von ursprünglich gültigen digitalen Signaturen weitgehend nutzlos, da sie ihre Gültigkeit von selbst über die Zeit verlieren. Entsprechend ist die nachfolgende Definition in Art. 3 aufzunehmen, welche sich an das deutsche Signaturgesetz anlehnt:

„Zeitstempel: Eine mit einer digitalen Signatur versehene digitale Bescheinigung einer Anbieterin von Zertifizierungsdiensten, dass ihr bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben."
Hier fehlen die Begriffe im Zusammenhang mit den notwendigen technischen Einrichtungen (Signaturerstellungseinheit /-prüfeinheit, vgl. Art. 2 EU-Richtlinie), vgl. Ziff. 4 und 5 der Vorbemerkungen.
Es fehlt auch der Begriff der „Relying Party", d.h. der Drittperson, welche ein digital signiertes Datenpaket erhält und dieses prüft.
Der Einsatz von Pseudonymen wäre vorteilhaft. Auf Grund verschiedener Diskussionen mit Vertretern der Wirtschaft kommen wir nichtsdestotrotz zum Schluss, dass die Integration in dieses Gesetz zum jetzigen Zeitpunkt nicht zwingend erforderlich ist.

321.04 Art. 4

Kantone / Cantons / Cantoni

BS Hier heisst es, dass im Handelsregister eingetragene natürliche und juristische Personen sowie Verwaltungseinheiten des Bundes, der Kantone oder der Gemeinden anerkannt werden können. Im Begleitbericht heisst es im Kommentar dazu unter Ziff. 210.021 Abs. 4 : „Ein Zertifizierungsanbieter muss im Handelsregister eingetragen sein, damit er anerkannt werden kann." Es ist nicht klar, ob dies auch für Verwaltungseinheiten gilt.

JU Selon le rapport explicatif, l'inscription obligatoire au registre du commerce n'est pas requise lorsque le fournisseur de services de certification qui demande à être reconnu est établi à l'étranger. Cette solution est susceptible de créer une inégalité de traitement au détriment des fournisseurs établis en Suisse ou y ayant une succursale ou une filiale.

NE Al. 1 Le projet prévoit que seules pourront être reconnues comme fournisseurs de services de certification les personnes physiques ou morales inscrites au registre du commerce, excluant par là même les personnes morales existantes sans inscription au registre du commerce. Il s'agit là d'une option qui paraît raisonnable, tant il est nécessaire pour l'utilisateur de la signature électronique de pouvoir connaître sans ambiguïté les partenaires avec lesquels il est appelé à travailler et qui apparaissent comme des tiers de confiance dans les rapports contractuels. Cette option doit donc être soutenue.
Let. f: Il paraît difficile de concevoir que pour être reconnu comme fournisseur de services de certification, il faille au préalable et avant d'être reconnu assurer que le droit qui sera applicable en la matière sera respecté. La finalité de cette disposition nous échappe à mesure qu'il nous paraît évident qu'un fournisseur de services de certification, une fois reconnu, doit prendre toutes les mesures nécessaires pour que le droit auquel il est soumis soit respecté, sous peine de perdre sa reconnaissance. Par contre, d'en faire une condition pour être reconnu relève de l'exploit impossible ou de la pétition de principe. Nous suggérons donc la rédaction suivante: *„s'engagent à* respecter le droit applicable en la matière".

TI Per garantire agli utenti la massima sicurezza, dovrà essere dedicata particolare attenzione e cura ai requisiti tecnici imposti per il riconoscimento dei prestatori di servizi di certificazione (art. 4). La diffusione della firma elettronica dipenderà dalla fiducia che gli utenti accorderanno a questo tipo di trasmissione dei dati. Di conseguenza le esigenze di sicurezza rivestono un'importanza primordiale.

VD Les let. a et f de l'al. 1 de cette disposition semblent inutiles, car elles renferment des évidences.
A propos de la let. d de l'al. 1, on peut relever, à titre comparatif, que le § 12 de la loi allemande (Gesetz zur digitalen Signatur – SigG) prévoit que tout fournisseur de service de certification doit constituer une provision d'un montant minimum de DM 500'000.-- en vue de couvrir les dommages éventuels engageant sa responsabilité. Les dispositions d'application de la loi sur la signature électronique devront à l'évidence contenir des règles semblables.
La page 16 du rapport explicatif mériterait quelques éclaircissements, car il y est mentionné que les cantons doivent prêter garde à des dispositions de droit public qui les empêcheraient d'être reconnus comme fournisseurs de services de certification.
La rédaction de l'al. 2 est malheureuse. En effet, cette disposition laisse entendre que les fournisseurs étrangers doivent être inscrits au registre du commerce, ce qui n'est pas le cas selon le rapport explicatif (page 16 du rapport explicatif). Nous vous proposons dès lors la rédaction suivante : *„les conditions prévues aux lettres a à f de l'alinéa 1 sont également valables pour les fournisseurs de services de certification étrangers qui n'ont ni filiale ni succursale en Suisse“*.

Parteien / Partis / Partiti

FDP Bei der Umsetzung der Zulassungsvoraussetzungen für in- und ausländische CA's ist darauf zu achten, dass deren Anerkennung in administrativ-formeller Hinsicht einfach und unkompliziert ausgestaltet wird (entsprechende Präzisierungen in den Ausführungsvorschriften nach Entwurf Art. 23).
Abs. 1 Bst. e: Der Intention der Pflicht zum Abschluss einer Haftpflichtversicherung ist zuzustimmen. Jedoch erscheint die Abschätzung der Höhe eines möglichen Schadens und damit der sinnvollen oder notwendigen Versicherungssumme aus der Anwendung von Art. 13 Abs. 2 und 3 des Entwurfs sehr schwierig. Eventuell wäre hier eine minimale Versicherungsdeckung vorzuschreiben, wie dies bei andern Berufsgattungen (z.B. Advokatur oder Notariat) üblich ist.
Abs. 2: Obwohl es sich aus dem textlichen Umkehrschluss sowie dem erläuternden Bericht (Ziff. 210.021 S. 17) ergibt, ist nicht für jeden Rechtssuchenden klar, dass für ausländische CA's der für die in der Schweiz ansässigen CA's notwendige Handelsregistereintrag nicht gelten soll. Im Interesse der Rechtssicherheit würden wir es begrüssen, Abs. 2 dementsprechend zu präzisieren.

SVP Als Zertifizierungsdiensteanbieter werden neben natürlichen und juristischen Personen des Privatrechts auch Verwaltungseinheiten des Bundes, der Kantone oder Gemeinden vorgeschlagen. Die SVP schlägt vor, die möglichen Zertifizierungsdiensteanbieter auf natürliche und juristische Personen, allenfalls auf die Kantone zu beschränken.

Organisationen / Organisations / Organizzazioni

Briner In Art. 4 lit. c ist unklar, was ganz konkret mit einem „zuverlässigen Informatiksystem“ gemeint ist, und was als „zuverlässiges Informatikprodukt“ gelten soll. Vom „zuverlässigen“ PC bis zum „zuverlässigen“ Drucker oder zur „zuverlässigen“ Datenbanksoftware ist es ein weiter Weg und eine weite Spanne.
Es sollte klarer gesagt werden, dass die hier genannten Voraussetzungen für die Anerkennung gegeben sein müssen, und dass diese Voraussetzungen aufrechterhalten werden müssen.

Regelungsbedürftig ist die Frage, was es für Folgen hat, wenn gewisse Voraussetzungen nicht erfüllt sein sollten. Nehmen wir an, eine Anbieterin von Zertifizierungsdiensten verwende keine „zuverlässigen Informatiksysteme und -produkte“, ohne dass das konkrete Auswirkungen auf die ausgestellten und verwalteten Zertifikate hat. Was sollen die Folgen sein? Auch der andauernde Versicherungsschutz (Art. 4 lit. e) ist zu gewährleisten; wer leistet Gewähr, dass die Versicherung auch wirklich Deckung bietet? Der Versicherungsschutz sollte wohl zu den zu publizierenden Informationen gehören.

Art. 4 lit. f regelt entweder eine Selbstverständlichkeit (nämlich dass man das anwendbare Recht einzuhalten habe) und ist dann zu streichen, oder aber stellt besondere Anforderungen, die klar(er) zu nennen sind.

CP Le projet prévoit toute une série de conditions qui sont tout à fait pertinentes. Cependant, nous estimons que les fournisseurs de services de certification ne doivent pas être des administrations fédérales, cantonales ou communales. Ce n'est pas le rôle de l'Etat de fournir de tels services à des tiers. Il doit se contenter de reconnaître les entreprises qui le font, vérifier qu'elles répondent aux critères légaux et respectent les obligations qui en découlent.

economiesuisse Gemäss Art. 4 können neben Privaten auch Verwaltungseinheiten des Bundes, der Kantone und Gemeinden als Anbieterinnen von Zertifizierungsdiensten anerkannt werden. Eine Konkurrenzierung von privaten Anbietern erachten wir als verfehlt, wenn es sich nicht um öffentliche Aufgaben handelt. Entsprechend müsste die Zulassung von Verwaltungseinheiten auf den Verkehr mit öffentlichen Stellen beschränkt werden. Im Privatverkehr sollen Verwaltungseinheiten als Anbieter von Zertifizierungsdiensten nicht aktiv werden.

Festzustellen ist ferner, dass ausländische Anbieter von Zertifizierungsdiensten nicht im Schweizer Handelsregister eingetragen sind. Der Klarheit halber muss Art. 4 angepasst werden.

FGSec Das Zertifikat sollte als „Qualified“ bezeichnet werden und die entsprechenden Eigenschaften aufweisen, da dies international verstanden wird, anstatt sich auf das BGES zu beziehen.

Zu Bst. c: Nicht nur zuverlässig, sondern auch vertrauenswürdig. Im deutschen Sprachgebrauch wird i.d.R. von „verlässlichen und vertrauenswürdigen Informationssystemen“ gesprochen.

Die Finanzmittel sollten ausreichen, damit der CSP arbeiten kann, ohne unangebrachte Rationalisierungen vornehmen zu müssen. Die Garantien und Versicherungen müssen ausreichen, um potentielle Haftung und Kosten der Stilllegung abdecken zu können. (Art. 13).

Zu Bst. d: Warum Finanzmittel *und* -garantien? Theoretisch sollte eines von beiden genügen.

Zu Bst. e: Es ist nicht klar, ob dies sowohl die Haftungsansprüche (Art. 18) wie auch die Kosten einer Stilllegung (Art. 13) betrifft. (e.g. *sowie* die Kosten...). Dies übersteigt die Anforderungen der EU-Direktive.

Es besteht ein prinzipielles Problem mit der „angemessenen Haftung” der Verwendung von Zertifikaten. Ein Zertifikat, welches auf unangemessenem Weg erlangt wurde, kann theoretisch tausendfach missbraucht werden, bevor es revoziert wird. Die Anzahl der Nutzungen liegt ausserhalb des Einflussbereichs des CSP’s oder des rechtmässigen Nutzers; deshalb kann er nicht dafür haften und es kann nicht durch ihn versichert werden.

FHZ Es ist sicherzustellen, dass jede schweizerische natürliche oder juristische Person einfach zu einer Anerkennung als CA nach Schweizer Recht kommt, falls

die Voraussetzungen des Art. 4 erfüllt sind. Es ist zu überlegen, ob nicht ein eigentlicher Rechtsanspruch auf Anerkennung als CA besteht.
Es ist sicherzustellen, dass die Anerkennung ausländischer CA's auch auf formell einfache Weise möglich ist. Vorarbeiten zur Anerkennung beispielsweise von Verisign sollten schon an die Hand genommen werden, damit die weltweit grossen CA's ab Inkrafttreten des Gesetzes anerkannt sind.
Die Details zu Art. 4 Abs. 1 sind in einer Verordnung genau zu regeln.
In Abs. 2 steht, dass ausländische Anbieterinnen die Voraussetzungen nach Abs. 1 zu erfüllen haben. Dies bezieht sich aber nur auf die Voraussetzungen von Art. 4 Abs. 1 lit. a - f. Dies ist zu präzisieren.
Die Voraussetzungen von Art. 4 Abs. 1 lit. e sind schwierig zu erbringen.
Die Ausstellung von Zertifikaten für den Eigengebrauch, wie es der Begleitbericht zum Entwurf für die Verwaltung vorsieht, scheint problematisch.

FRI L'art. 4 énumère une série de conditions cumulatives permettant d'obtenir une reconnaissance en tant que fournisseur de services de communication. Celles-ci nous semblent justifiées dès lors que les organismes reconnus doivent être dignes de confiance et qu'ils agissent au cœur même de toute l'organisation mise en place.
En revanche, le fait de prévoir que les unités administratives de la Confédération, des cantons ou des communes puissent être reconnues nous paraît très contestable. Le rôle de l'Etat ne consiste pas à fournir de tels services, mais doit se cantonner à reconnaître les entreprises sélectionnées et vérifier le strict respect des obligations légales qui en découlent.

FSP A ce sujet, nous avons retenu que la validité de la signature électronique est garantie par l'intervention de tiers de confiance appelés „fournisseurs de services de certification reconnus“, dont le travail consiste à vérifier l'identité du titulaire d'une clé privée et à établir le lien avec le titulaire de la clé publique correspondante.
A notre avis cependant, les conditions posées pour la reconnaissance des fournisseurs de services fixées à l'art. 4 du projet ne sont pas claires et confèrent un pouvoir trop large au Conseil fédéral.
En effet, les conditions posées par la loi pour la reconnaissance des fournisseurs de service de certification nous paraissent essentielles au fonctionnement même du système que souhaite mettre en place le projet de loi sur la signature électronique.
Les dispositions concrétisant ces exigences devraient donc être contenues dans la loi et non, comme le prévoit le projet, dans une ordonnance.
S'agissant des obligations (financières, techniques, organisationnelles) incombant aux fournisseurs de services de certification, notre Fédération constate que l'application concrète de la loi fédérale sur la signature électronique exige la mise en place de tout un arsenal de mesures de surveillance. Une telle infrastructure est particulièrement coûteuse d'autant plus que son efficacité nous paraît pour le moins sujette a caution.
En plus des exigences exposées ci-dessus, les fournisseurs de certification doivent se prémunir contre „certains risques“ (cf. page 16 du rapport explicatif) au moyen d'une assurance.
A ce sujet, notre Fédération n'a trouvé ni dans le rapport explicatif, ni dans la lettre même du projet, la réponse à la question de savoir quelles sont les assurances qui accepteront d'assurer ces fournisseurs de certification sans pouvoir évaluer le risque qu'elles pourraient être amenées à couvrir.

kf Wir erachten es nur als sinnvoll, dass *„...Verwaltungseinheiten des Bundes, der Kantone oder der Gemeinde...“* auch anerkannt werden können, wenn es sich um öffentliche Aufgaben handelt.
Nach unserer Information können ausländische Anbieter ohne Sitz in der Schweiz nicht im Handelsregister eingetragen werden. Wir wünschen deshalb die entsprechende Korrektur unter Abs. 1.

SBV Dans la mesure où un fournisseur de services de certification remplit les conditions fixées à l'art. 4 al. 1, il devrait être assuré d'être reconnu. Nous proposons dès lors de modifier cette disposition comme suit:
„ *Sont* reconnus comme fournisseurs de services de certification…“
„Als Anbieterinnen von Zerifizierungsdiensten *werden anerkannt* …:“
Afin de clarifier la position des fournisseurs de services de certification étrangers par rapport aux fournisseurs suisses, nous proposons de modifier comme suit l'al. 2 :
„*A l'exception de l'inscription au registre suisse du commerce,* les conditions prévues à l'alinéa 1 sont également valables pour les fournisseurs de services de certification étrangers…“
„*Abgesehen vom Erfordernis eines Handelsregistereintrages in der Schweiz gelten die Voraussetzungen nach Absatz 1* auch für ausländische Anbieterinnen von Zertifizierungsdiensten.“
Par ailleurs, le projet de loi pourrait reprendre, à l'art. 8, les conditions fixées dans l’annexe 2 de la directive européenne sur un cadre communautaire pour les signatures électroniques. La fixation d’exigences analogues à celles de la directive serait susceptible de faciliter ultérieurement la reconnaissance des fournisseurs suisses de services de certification dans les pays de l’Union européenne.

SWICO Für ein klareres Verständnis in bezug auf die Unterschiede zwischen Abs. 1 und Abs. 2 würden wir es als sinnvoll erachten, den Abs. 2 durch den nachfolgenden Wortlaut zu ersetzen: *„Abgesehen vom Erfordernis eines Handelregistereintrages in der Schweiz gelten die Voraussetzungen nach Absatz 1 auch für ausländische Anbieterinnen von Zertifizierungsdiensten.“*

SwissICT Damit die Kompatibilität der elektronischen Signatur mit der europäischen Rechtsprechung hergestellt wird, fordert SwissICT als grösster Branchenvertreter im Bereich der Informations- und Kommunikationstechnologie im Rahmen des Vernehmlassungsverfahrens Richtlinien zur Vereinheitlichung der Anforderungen an die Zertifizierungsdiensten sowie Regeln zur Anerkennung von Signaturen im internationalen Umfeld.

Schlauri/Kohlas Die in Art. 4 Abs. 1 Bst. a genannte Anforderung, die Zertifizierungsdiensteanbieter müssten in der Lage sein, die Zertifikate gemäss den Anforderungen des BGES zu erfüllen, ist bereits Teil der in Bst. f genannten Anforderung, die Zertifizierungsdiensteanbieter müssten die Einhaltung des anwendbaren Rechts gewährleisten. Bst. a kann daher gestrichen und die Formulierung von Bst. f nach vorne zu Bst. a verschoben werden.
Art. 4 Abs. 2 ist missverständlich formuliert. Aus dem vorgeschlagenen Wortlaut könnte e contrario gefolgert werden, die Voraussetzungen von Abs. 1 würden für ausländische Zertifizierungsdiensteanbieter mit Haupt- oder Zweigniederlassung in der Schweiz nicht gelten, sie könnten also auch ohne deren Erfüllung anerkannt werden. Sinn der Regelung ist jedoch, von ausländischen Anbietern keinen Handelsregistereintrag zu verlangen, sofern sie einen solchen mangels eintragungsfähiger Niederlassung nicht erhalten können.

Die Differenzierung zwischen Haupt- und Zweigniederlassung kann ferner mangels unterschiedlicher Rechtsfolge unterbleiben.
Aus diesen Gründen ergibt sich der folgende Formulierungsvorschlag für Art. 4 Abs. 2. Die Variante 2 mit Beschränkung auf Personen würde ausländische Verwaltungseinheiten e contrario ausschliessen, was in Variante 1 unklar bleibt.
„[2]Ausländische [1) Anbieter von Zertifizierungsdiensten][2) Personen] können unter den Voraussetzungen von Abs. 1 auch ohne Handelsregistereintrag [2) als Anbieter von Zertifizierungsdiensten] anerkannt werden, sofern sie in der Schweiz nicht über eine eintragbare Niederlassung verfügen."

321.05 Art. 5

Kantone / Cantons / Cantoni

AI Leider spricht sich die Vernehmlassungsvorlage nicht darüber aus, wer als Anbieter und Kontrollstelle (Akkreditierungsstelle) von Zertifizierungsdiensten vorgesehen ist.

BS Unter Ziff. 210.022 heisst es im Begleitbericht nicht eindeutig und klar : „Die Anerkennung ist keine Verfügung." - sondern : „Die Anerkennung gilt nicht als Verfügung." Unter Ziff. 210.09 wiederholt sich das. Heisst das, dass die Anerkennung zwar eine Verfügung ist, aber doch nicht als Verfügung gilt? Wenn die Anerkennung keine Verfügung ist, warum schreibt man das nicht einfach so hin? Warum der Umweg über das ‚nicht gelten'?
Gemäss Art. 5 Abs. 1 bezeichnet der Bundesrat die für die Akkreditierung zuständige Akkreditierungsstelle. Die Akkreditierungsstelle akkreditiert die Anerkennungsstelle. Die Anerkennungsstelle anerkennt die Anbieterinnen von Zertifizierungsdiensten.
Im Kommentar zum Artikel 5 wird unter Ziff. 210.022 des Begleitberichts ausgeführt, dass es sich bei der Anerkennung der Anbieterinnen von Zertifizierungsdiensten durch die Anerkennungsstelle um ein privatrechtliches Rechtsgeschäft handelt und dass die Anerkennung nicht als Verfügung im Sinne von Art. 5 VwVG gilt. Anderseits heisst es unter Ziff. 31 des Begleitberichtes, dass das Bundesgesetz die Grundlage für die „staatliche Anerkennung" von Zertifizierungsdiensteanbieterinnen schafft und dass die damit verbundenen Aufwendungen - über Gebühren - von den Anerkennungsstellen und den Zertifizierungsdiensteanbieterinnen zu tragen sind, wo auch der Begriff der „Gebühr" wiederum auf eine Verfügung hinweist.
Das Verhältnis zwischen Bundesrat und Akkreditierungsstelle und das Verhältnis zwischen Akkreditierungsstelle und Anerkennungsstelle ist nach unserer Beurteilung öffentlichrechtlich. Dafür spricht unseres Erachtens, dass gemäss Art. 21 Abs. 2 das zuständige Departement die Gebühr für die von der Akkreditierungsstelle abzugebende Bestätigung festlegt - der Begriff der Gebühr wird mit einer Gegenleistung für eine staatliche Leistung in Verbindung gebracht - und dass gemäss dem Kommentar dazu es sich um eine „offizielle" Bestätigung handelt. Bei dieser „offiziellen" Bestätigung handelt es sich u.E. um eine Verfügung. Im Kommentar zu Art. 21 heisst es im Begleitbericht unter Ziff. 210.09 dazu, dass die Bestätigung nicht als Verfügung gilt, da sie weder Rechte noch Pflichten der Antragsteller statuiert, sondern einzig und allein einen Sachverhalt feststellt. Damit könnte sie aber immer noch eine Feststellungsverfügung sein. Ist die Bestätigung aber keine Verfügung, dann ist sie auch nicht offiziell, und dann ist für die Ausstellung der Bestätigung nicht eine „Gebühr" zu erheben, sondern ein „Preis" zu verlangen.

Erst wenn klar ist, ob ein öffentlichrechtliches oder ein privatrechtliches Verhältnis vorliegt, ist auch klar, ob das Entgelt für eine Leistung eine Gebühr ist oder ein Preis. Unter Ziff. 31 des Begleitberichtes heisst es, dass die Aufwendungen - über Gebühren - von den Anerkennungsstellen und den Zertifizierungsdiensteanbieterinnen zu tragen sind, die um Akkreditierung oder um Anerkennung nachsuchen. Wenn diese Entgelte tatsächlich Gebühren sind, dann braucht es für die Erhebung der Gebühren eine gesetzliche Grundlage. Im ganzen Gesetzesentwurf haben wir aber keine gesetzliche Grundlage für die Gebührenerhebung gefunden.
Wenn gemäss Art. 21 Abs. 3 eine andere Stelle eine Bestätigung im Sinne von Art. 21. Abs. 1 abgibt, stellt sich die gleiche Frage, ob es sich dann um eine Verfügung oder um eine private Erklärung handelt.
Wenn der Bundesrat gestützt auf Art. 5 Abs. 2 die Akkreditierungsstelle auch als Anerkennungsstelle bezeichnet, ist dann das Verhältnis zwischen der als Anerkennungsstelle agierenden Akkreditierungsstelle und den um Anerkennung nachsuchenden Anbieterinnen von Zertifizierungsdiensten privatrechtlich oder öffentlichrechtlich, und woran erkennt man, ob es das eine oder das andere ist ? Unseres Erachtens sollte das Gesetz so klar sein, dass sich diese Fragen gar nicht stellen oder dass das Gesetz sie eindeutig beantwortet.
Der Entwurf schliesst nicht aus, dass auch Strafverfolgungsbehörden, welche die Dienste der Akkreditierungsstelle in Anspruch nehmen, eine Gebühr oder Preise bezahlen müssten. Diese Auswirkung sollte unbedingt vermieden werden; die Erfahrungen mit Randdatenerhebungen und Telephonkontrollen via UVEK haben gezeigt, welche enormen Summen die Strafjustiz bei Ermittlungen im Telekommunikationsbereich ausgeben muss. Die Gebühren oder Preise der Akkreditierungsstelle müssten so kalkuliert werden, dass Behörden die in Frage stehenden Bestätigungen kostenlos erhalten können. Es wäre nicht zu verstehen, wenn das Spezialkommando, das nach einer Bombendrohung in einem Kino die Bombe sucht und entschärft, noch einen Kinoeintrittspreis bezahlen müsste.
Es ist hier daran zu erinnern, dass unter Ziff. 31 im Begleitbericht ausgeführt wird, dass die öffentliche Hand nur geringfügig in den sachgerechten Vollzug des Bundesgesetzes über die elektronische Signatur involviert ist, und dass die damit verbundenen Aufwendungen über Gebühren von den Anerkennungsstellen und den Zertifizierungsdiensteanbieterinnen zu tragen sind, die um Akkreditierung oder Anerkennung nachsuchen. Es ist nicht einzusehen, warum Strafverfolgungsbehörden, die durch ihre Tätigkeit zum einwandfreien Vollzug des Bundesgesetzes beitragen und den unter Ziff. 32 des Begleitberichtes erwähnten rechtssicheren und vertrauensbildenden Rahmen für den elektronischen Geschäftsverkehr schaffen, dafür noch mit Kosten belastet und bestraft werden sollen.
Aus den folgenden Bestimmungen geht hervor, dass es sich um „*Anerkannte* Anbieterinnen von Zertifizierungsdiensten“ handelt.

SG Wir beantragen, in Art. 5 Abs. 1 den ersten Satz zu streichen und den Randtitel von Art. 5 wie folgt zu formulieren: „Bezeichnung der Anerkennungsstelle“.
Begründung: Vgl. unsere Begründung zu Art. 3 Bst. h (neu).

TI Il servizio di accreditamento preposto al riconoscimento dei prestatori di servizi di certificazione (art. 5) deve disporre delle risorse necessarie (in mezzi tecnici e personale qualificato) per garantire agli utenti un servizio ineccepibile e la massima sicurezza compatibile con la trasmissione elettronica di dati, per sua natura soggetta a rischi ben noti (virus, sovraccarico di linee, pirateria ecc.).

VD L'on ne comprend pas la référence au „droit de l'accréditation“ figurant à la première phrase du premier alinéa de cette disposition.

VS Selon le rapport, la reconnaissance des fournisseurs de services de certification (section 2, art. 4 ss) est un acte juridique de droit privé de sorte qu'un litige portant sur ce point relève de la compétence du juge civil. La solution paraît peu appropriée à la spécificité du problème à dominante technique, scientifique. Outre les lenteurs de la procédure civile, il est certain que le juge devra ordonner une expertise. Ne conviendrait-il pas de considérer que les organismes de reconnaissance exercent une tâche de droit public et délivrent ou refusent une autorisation de police, en d'autres termes qu'ils rendent une décision administrative sujette à recours auprès d'une commission spécialisée ?

ZG Der Begriff „Akkreditierungsrecht“ in Art. 5 kann zu Missverständnissen führen. Gibt man beispielsweise auf der Internetseite des Bundes diesen Suchbegriff ein, verweist das Internet nur auf diesen Vernehmlassungsentwurf. In der publizierten SR findet man unter „Akkreditierung“ die Verordnung über die Akkreditierung von Journalisten aus dem Jahr 1990 (SR 170.6). Und dieses Akkreditierungsrecht kann damit sicher nicht gemeint sein. Wir regen an, diesen Begriff nochmals zu prüfen. Gleiches gilt für den Inhalt von Art. 5 Abs. 1. Diese Aussage verwirrt. Im Bericht wird dazu erwähnt, es sei ein einfaches und transparentes Regime für die Anerkennung vorzusehen.

<u>Organisationen / Organisations / Organizzazioni</u>

camera commercio L'art. 5 regola la questione del riconoscimento dei prestatori di servizi di certificazione. Secondo il rapporto esplicativo, l'articolo va interpretato nel senso che un prestatore accreditato all'estero non può certificare un prestatore di servizi di certificazione svizzero, nel caso in cui venga richiesto un riconoscimento svizzero. A nostro avviso, l'articolo 5 andrebbe modificato, in modo tale da non escludere a priori la possibilità di una collaborazione con prestatori di servizi di certificazione stranieri, collaborazione che potrebbe essere basata su un certificato di base comune. E' in effetti difficile prevedere quali modelli di „Trust“ possano svilupparsi nel futuro prossimo. Siamo quindi dell'opinione che la Svizzera non dovrebbe auto-limitarsi, rendendo non conformi alla nuova legge federale sulla firma digitale le strutture di chiavi pubbliche internazionali che si stanno creando nel mondo bancario internazionale. Si tratta di un elemento importante se si vuole ottenere un riconoscimento svizzero delle firme digitali legate a detta evoluzione internazionale.

CP L'articulation de la surveillance nous semble poser problème, en raison de l'opacité des art. 5 et 15 du projet. A leur lecture, on comprend que le système est à 4 étages puisqu'il met en scène les acteurs suivants : les fournisseurs de services de certification, ceux d'entre eux qui sont reconnus, les organismes d'accréditation et enfin l'Etat.

Nous ne saisissons pas pourquoi les organismes de reconnaissance doivent en principe être distincts des organismes d'accréditation. L'art. 5 al. 2 du projet donne d'ailleurs à penser que la séparation n'est pas inéluctable. En tout état de cause, le système tel qu'il est prévu apparaît lourd et compliqué, desservi en outre par une médiocre rédaction des articles de loi.

DigiSigna Wie / Comme / Come Camera commercio.

economiesuisse Gemäss dem Begleitbericht zum Entwurf geht aus Art. 5 (bez. Anerkennungsstelle) hervor, dass Zertifizier-Hierarchien ausgeschlossen sind. Es wird auf Nachteile hingewiesen. Diese werden aber nur insofern

spezifiziert, dass die Kontrolle der Tätigkeit schwieriger ist. Welche Modelle von internationalen Public Key Infrastrukturen sich durchsetzen werden, ist unseres Erachtens offen. Es ist immerhin darauf hinzuweisen, dass grosse hierarchisch organisierte internationale Public Key Infrastrukturen (z.B. Identrus oder GTA der internationalen Bankenwelt) dadurch vom Geltungsbereich des BGES ausgeschlossen werden. Dies dürfte für die Verarbeitung der digitalen Signatur gemäss BGES nicht förderlich ein. Es ist auch nicht einzusehen, weshalb in einer internationalen Hierarchie nicht verschiedene staatliche Anerkennungen stattfinden können.

FHZ Die Anerkennungsstellen sollten verpflichtet werden, von sich aus auf ausländische CA's zuzugehen, um deren Anerkennung sicherzustellen.

FRI Vgl. zu Art. 2 / Cf. ad art. 2 / Cfr. ad art. 2.

FSP La procédure fixée par le projet pour la reconnaissance d'un fournisseur de services de certification nous paraît compliquée et le rapport est muet sur la question de savoir si les mesures de contrôle prévues seront vraiment efficaces. Sans cette garantie, nous émettons les plus grandes réserves sur cette procédure.

ISACA Les conditions de reconnaissance des fournisseurs de service de certification sont détaillées à l'art. 4. Rien de tel pour les organismes de reconnaissance, dont les tâches de surveillance des fournisseurs sont cependant importantes (voir l'art. 15/1 notamment). L'introduction d'une condition telle que „emploient du personnel possédant les connaissances, l'expérience et les qualifications nécessaires (cf. let. b de l'art. 4/1)" est notamment indispensable. Enoncer à l'art. 5 les conditions de reconnaissance des organismes de reconnaissance.

KPMG Wir schlagen vor, die Rechtsbeziehung zwischen der Anerkennungsstelle und den Anbieterinnen von Zertifizierungsdiensten - insbesondere die Frage der Ablehnung von Gesuchstellern - nochmals zu prüfen.

Am 12. April 2000 erliess der Bundesrat die Verordnung über die Dienste der elektronischen Zertifizierung und setzte sie auf den 1. Mai 2000 in Kraft. Die ZertDV war als Versuchsverordnung konzipiert und zeitlich befristet. Bei Erlass der ZertDV war vorgesehen, dass ein Bundesgesetz eingeführt wird, das anstelle der ZertDV treten soll.

Der ZertDV wurde im Rahmen ihrer Ausarbeitung das sog. Root-System zu Grunde gelegt. Das BAKOM sollte in einem hierarchischen System die digitalen Signaturen der Zertifizierungsdienstanbieter zertifizieren. Dieses System, welches in Anlehnung an das deutsche System vorgeschlagen wurde, wurde in der Folge aufgrund grosser Kritik im Vernehmlassungsverfahren zur ZertDV fallen gelassen. Stattdessen wurde das System einer freiwilligen staatlichen Akkreditierung und Anerkennung gewählt (LEGLER Thomas, Electronic Commerce mit digitalen Signaturen in der Schweiz, Bern 2001, S. 9.).

Das Annerkennungssystem ist hierarchisch geordnet. Gemäss Art. 5 der Akkreditierungs- und Bezeichnungsverordnung (AkkBV SR 946.512) betreibt das Eidgenössische Amt für Messwesen die Schweizerische Akkreditierungsstelle (SAS). Diese beantragt bei EJPD Gutheisssung/Ablehnung des Akkreditierungsgesuchs der Anerkennungsstellen (Art. 5 E-BGES). Diesen Anerkennungsstellen obliegen ihrerseits die Anerkennung (Art. 5 E-BGES) und Beaufsichtigung (Art. 15 E-BGES) der Anbieterinnen von Zertifizierungsdiensten.

Wir würden es - im Interesse der Übersichtlichkeit - begrüssen, wenn das E-BGES in einer Fussnote zu Art. 5 auf das Bundesgesetz über die technischen

Handelshemmnisse (THG: SR 946.51) und das AkkBV verweisen würde (nicht nur bei Art. 15). Ferner sind wir der Meinung, dass in der Botschaft des Bundesrates zum E-BGES die erwähnten Rechtsgrundlagen noch etwas stärker betont und der Zusammenhang mit dem E-BGES noch eingehender umschrieben werden sollten.
Auf der Grundlage dieses Systems wird ein Zertifizierungsdienstanbieter von einer Anerkennungsstelle anerkannt, die wiederum von einer Akkreditierungsstelle akkreditiert wird.
Die Akkreditierung der Anerkennungsstellen wird durch die AkkBV umschrieben. Das Rechtsverhältnis zwischen der Akkreditierungsstelle und Anerkennungsstelle ist hoheitlicher, d.h. öffentlich-rechtlicher Natur.
Mit der Akkreditierung oder der Bezeichnung überträgt der Bund den betreffenden Stellen keine hoheitlichen Befugnisse. Die akkreditierten oder bezeichneten Stellen bleiben verantwortlich für ihre Tätigkeit, insbesondere für die von ihnen ermittelten Prüfergebnisse und ausgestellten Konformitätsbescheinigungen (Art. 35 AkkBV).
Demnach ist die Rechtsbeziehung zwischen Anerkennungsstelle und Zertifizierungsdienstanbieter privatrechtlicher Natur. Diesen Grundsatz hält auch der Bericht 2001 zum Entwurf des Bundesgesetzes über die elektronische Signatur fest: „Die Anerkennung ist ein privatrechtliches Rechtsgeschäft. Sie gilt nicht als Verfügung im Sinne von Artikel 5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG; SR 172.021). Mögliche Streitigkeiten zwischen Anerkennungsstellen und anerkannten oder nicht anerkannten Anbieterinnen von Zertifizierungsdiensten unterliegen nicht der Verwaltungsrechtspflege, sondern werden von den Zivilgerichten entschieden.“ (Bericht 2001, S. 17)
Für die Anerkennung der Anbieterinnen von Zertifizierungsdiensten zuständig sind Stellen (Anerkennungsstellen), die nach dem Akkreditierungsrecht dafür akkreditiert sind (Art. 5 Abs. 1 E-BGES). Fehlt eine Anerkennungsstelle, so kann der Bundesrat die Akkreditierungsstelle auch als Anerkennungsstelle bezeichnen (Art. 5 Abs. 2 E-BGES).
Da einer Anerkennungsstelle mit dem heutigen Entwurf keine hoheitlichen Befugnisse erteilt werden, trifft sie auch keine Pflicht, einen Bewerber anzuerkennen (Die Allgemeinen Anforderungen an Stellen, die Qualitätsmanagementsysteme begutachten und zertifizieren (EN 45012; ISO 62), sehen zwar vor, dass Gesuche von Zertifizierungsdienstanbieter nur aus wichtigen Gründen abgelehnt werden dürfen. Dies bedeutet eine Abweichung von der Vertrags- bzw. Partnerwahlfreiheit und sollte deshalb eine Rechtsgrundlage im BGES finden). Die Anerkennungsstelle verfügt hier über eine Partnerwahlfreiheit. Auch der Wortlauf von Art. 4 E-BGES lässt darauf schliessen, dass der Bewerber keinen Anspruch auf Anerkennung hat, selbst wenn er alle Voraussetzungen zur Anerkennung erfüllt. Diese Sachlage könnte unmittelbar nach Inkrafttreten des BGES problematisch sein, nämlich dann, wenn in einer Anfangsphase nur eine Anerkennungsstelle existiert, die dann praktisch über eine Monopolstellung verfügt. Der Gang zu einem Zivilgericht trägt dieser Problematik keine Rechnung, da der Bewerber keinen gesetzlichen Anspruch auf Anerkennung hat.
In diesem Zusammenhang möchten wir einzig die Frage aufwerfen, ob diese Rechtslage dem Zweck des Gesetzes entspricht, oder ob das Gesetz nicht Voraussetzungen schaffen sollte - im Interesse des Marktplatzes Schweiz -, die Zertifizierung als eine Art „Service Public“ anzuerkennen? Ein anderer Lösungsansatz wäre jener gemäss Krankenkassenversicherung. Hier ist das Rechtsverhältnis zwischen Bund und Krankenkassen ein hoheitliches, das

Rechtsverhältnis zwischen Krankenkasse und Versichertem demgegenüber privatrechtlicher Natur. Sobald hingegen eine Krankenkasse auf einen Antrag eines Versicherten ablehnend reagiert, hat sie ihren Entscheid in Form einer Verfügung zu erlassen, die der betroffene Versicherte auf dem Verwaltungsrechtspflegeweg weiterziehen kann.

Muster/Sury Im Gesetz wird nicht geregelt, wer Anerkennungsstelle für die Anbieter von elektronischen Zertifikaten sein kann und welche Bedingungen diese Anerkennungsstellen dazu erfüllen müssen. Im Gesetz nicht klar geregelt ist, welche Rechtsform/rechtliche Wirkung die Akkreditierung als solche hat. Dies ist sehr wichtig, da der Überwachung der Zertifizierungsstelle zwecks Verhinderung von Schäden (begangen aus Absicht oder Fahrlässigkeit) in Zukunft eine grosse Verantwortung für die Wirtschaft und die Rechtssicherheit zukommt.

In Zukunft wird sich der Gebrauch der Zertifikate verbreiten. Dadurch werden die möglichen Schäden oder Risiken bei Missbrauch oder fehlerhaftem Erstellen der Zertifikate enorm zunehmen. Somit kommt der Zertifizierungsstelle in Zukunft eine zentrale volkswirtschaftliche Bedeutung zu. Es wäre wünschenswert, dass die Erlaubnis für das Anbieten von Zertifikaten verwaltungsrechtlich einer Polizeierlaubnis gleichkommt, wie bei Banken und Versicherungen.

Weiter sollten die Höhe der finanziellen Mittel und Garantien und andere Anforderungen in diesem Gesetz möglichst auf Gesetzesstufe geregelt werden.

SUISA Für den Dualismus von Anerkennungsstellen und Akkreditierungsstelle haben wir nirgends eine einleuchtende Begründung gefunden. Dass die Anbieter von Zertifizierungsdiensten - betrachtet man ihre Aufgaben und ihre Haftung - anerkannt und beaufsichtigt werden müssen, ist notwendig. Dass diese Tätigkeiten jedoch auf zwei Stellen aufgeteilt werden sollen, erscheint uns als unnötige Doppelspurigkeit. Wir halten Anerkennung und Beaufsichtigung der Zertifizierungsdienste für eine genuin staatliche Aufgabe. Eine allfällige Abweichung zum europäischen Recht kann in diesem Punkt ohne weiteres in Kauf genommen werden.

SWICO Gemäss Erläuterungen (S.17) soll es sich bei der Akkreditierung um ein privatrechtliches Rechtsgeschäft handeln, was letztlich nicht einleuchtend ist (vgl. hierzu etwa auch Art. 15, Entzug der Anerkennung).

Treuhandkammer Die Akkreditierung der Anerkennungsstellen ist in der Verordnung über das schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitätsbewertungs-, Anmelde- und Zulassungsstellen (AkkBV) umschrieben und ist hoheitlicher, d.h. öffentlich-rechtlicher Natur. Demgegenüber untersteht die Rechtsbeziehung zwischen Anerkennungsstelle und Zertifizierungsdienstanbieter dem Privatrecht. Dies hält der Begleitbericht zum Entwurf zu einem Bundesgesetz über die elektronische Signatur („Begleitbericht“, S. 17) fest: „Die Anerkennung ist ein privatrechtliches Rechtsgeschäft. Sie gilt nicht als Verfügung im Sinne von Artikel 5 des Bundesgesetzes über das Verwaltungsverfahren. Mögliche Streitigkeiten zwischen Anerkennungsstellen und anerkannten oder nicht anerkannten Anbieterinnen von Zertifizierungsdiensten unterliegen nicht der Verwaltungsrechtspflege, sondern werden von den Zivilgerichten entschieden.“

Sofern sich ein Unternehmen als Zertifizierungsdienstanbieter anerkennen lassen will, muss es sich mit einem Gesuch um Anerkennung an eine Anerkennungsstelle wenden (Art. 5 Abs. *2* E-BGES). Fehlt eine Anerkennungsstelle, so kann der Bundesrat die Akkreditierungsstelle auch als Anerkennungsstelle bezeichnen (Art. 5 Abs. *2* E-BGES).

Mit dem Entscheid, das Rechtsverhältnis zwischen Anerkennungsstelle und Zertifizierungsdienstanbieter dem Privatrecht zu unterstellen, gilt für die Anerkennungsstelle die Vertragsfreiheit, d.h. unter anderem auch die Partnerwahlfreiheit. Auch der Wortlaut in Art. 4 E-BGES lässt darauf schliessen, dass der Gesuchsteller keinen Anspruch auf Anerkennung hat, selbst wenn er alle gesetzlichen Voraussetzungen zur Anerkennung erfüllt. Diese Sachlage könnte unmittelbar nach Inkrafttreten des BGES zu Problemen führen, nämlich dann, wenn in einer Anfangsphase nur eine Anerkennungsstelle existiert, die dann praktisch über eine Monopolstellung verfügt. Der Gang zu einem Zivilgericht trägt dieser Problematik keine Rechnung, da der Bewerber keinen gesetzlichen Anspruch auf Anerkennung hat.
In diesem Zusammenhang möchten wir die Frage aufwerfen, ob diese Rechtslage dem Zweck des Gesetzes entspricht, oder ob das Gesetz nicht Voraussetzungen schaffen sollte - im Interesse des Marktplatzes Schweiz - die Zertifizierung als eine Art „Service Public“ anzuerkennen? Wäre hier, wenigstens solange nicht mehrere Anerkennungsstellen auf dem Markt sind, eventuell eine Anerkennungspflicht, ähnlich der Transportpflicht gemäss Art. 3 Transportgesetz, sinnvoll? Ein anderer Lösungsansatz wäre jener gemäss Krankenversicherungsgesetz (KVG). Hier ist das Rechtsverhältnis zwischen Bund und Krankenkassen ein hoheitliches, das Rechtsverhältnis zwischen Krankenkasse und Versichertem demgegenüber privatrechtlicher Natur. Sobald hingegen ein Versicherer mit einem Entscheid der Krankenkasse nicht einverstanden ist, kann er verlangen, dass sie ihren Entscheid in Form einer Verfügung erlässt (Art. 80 KVG), die der betroffene Versicherte auf dem Verwaltungsrechtspflegeweg weiterziehen kann.
Im übrigen verweisen wir auf die Stellungnahme des SWICO zu Art. 5.

321.06 Art. 6

Kantone / Cantons / Cantoni

NE Puisqu'il a été renoncé à toute publication dans la Feuille fédérale ou dans la Feuille officielle suisse du commerce des fournisseurs de services de certification reconnus, le public devrait pouvoir obtenir sur demande et gratuitement cette liste, ne serait-ce que par Internet, liste qui devrait être mise systématiquement et journellement à jour pour éviter une distorsion de concurrence.

VD Vu son importance, la liste des fournisseurs de services de certification reconnus devrait être officiellement publiée, sa seule mise à disposition du public, prévue à l'al. 2, ne paraissant pas suffisante.

VS La question d'une publication de la liste des fournisseurs de services de certification reconnus mériterait un examen (art. 6 al. 2).

Parteien / Partis / Partiti

PLS Des mesures techniques devraient être prévues pour éviter que la liste des fournisseurs puisse être modifiée de manière indue.

Organisationen / Organisations / Organizzazioni

FRC Nous demandons l'adjonction suivante: *„Cette liste doit être accessible en tout temps et mise à disposition gratuitement pour les consommateurs“.*

KVN Im Interesse der Konsumentenschaft sollte hier genauer definiert werden, wie, wann und wo die Akkreditierungsstelle die Liste der anerkannten Anbieterinnen von Zertifizierungsdiensten zur Verfügung stellt.

SBV Il y a lieu de garantir, par des mesures techniques appropriées, que la liste des fournisseurs de services de certification ne puisse être indûment modifiée. L'art. 6 devrait être modifié dans ce sens.

SWICO Authentisierung: Es muss technisch sichergestellt werden, dass die Liste, auf die elektronisch zugegriffen wird, ebenfalls authentisch ist. Eben eine solche Regelung fehlt jedoch (auch gehört sie wohl nicht in die technischen Ausführungsbestimmungen).

321.07 Art. 7

Kantone / Cantons / Cantoni

AR Ungewissheiten bestehen bezüglich der Langzeit-Eigenschaften der ganzen Public-/Private-Key Technologie. Wenn die Technologie sich so schnell wie bisher weiter entwickelt, werden auch heute als sicher geltende Schlüsselalgorithmen bald nicht mehr unauflösbar sein.
In diesem Zusammenhang muss darauf hingewiesen werden, dass der technische Wandel die Zertifikate rasch überholen könnte. Die Frage der elektronischen Identifikation eines Absenders könnte sich daher in rascher Folge immer wieder stellen. Damit bleibt aber auch offen, wie in zehn oder mehr Jahre Schlüssel von heute verifiziert werden können. Die gleichen Fragen stellen sich, wenn die Anbieter von Zertifizierungsdiensten vom Markt verschwinden.

Organisationen / Organisations / Organizzazioni

economiesuisse Abs. 2 ist ersatzlos zu streichen. Diese Bestimmung steht mit identischem Wortlaut bereits in Art. 23 Abs. 2, wo sie von der Systematik her auch hingehört.

FHZ Der Bundesrat soll die Generierung kryptografischer Schlüssel regeln. Nebst der technischen Hintergründe könnten vielleicht Staatsschutzinteressen das Motiv sein. Die entsprechende gesetzliche Grundlage ist hier zu legen resp. darauf zu verweisen.

FRC Le projet du Conseil fédéral n'a pas repris la Directive européenne 1999/93/CE qui distingue, d'une part, les dispositifs de création de signature et les dispositifs sécurisés de création de signature et, d'autre part, le certificat et le certificat qualifié.
Pour des raisons de clarté, la FRC demande impérativement l'adjonction suivante: *„Seules les signatures électroniques basées sur un certificat qualifié et créées par des dispositifs sécurisés sont assimilées à la signature manuscrite*“.
Un système d'horodatage (Zeitstempel) qualifié avec une certification qualifiée portée sur la signature électronique est prévu afin de permettre aux consommateurs d'apporter la preuve d'une utilisation abusive de leur clé privée par exemple.

FSP La loi veut établir un système de contrôle permanent des clés délivrées. Nous nous demandons cependant de quelle façon concrète ce contrôle pourra se dérouler, dès lors que ni le projet ni le rapport ne nous fournissent des explications suffisantes à ce sujet.
Nous demandons aux autorités fédérales de fixer correctement, par voie d'ordonnance ou par tout autre moyen idoine, les modalités de ce contrôle. Dans le cas contraire, les dispositions y relatives pourraient bien rester lettre morte.

kf Streichen. Wird nochmals unter Art. 23 Abs. 2 erwähnt, das genügt nach unserer Ansicht.

Muster/Sury Es ist durchaus begrüssenswert, dass der Bundesrat die Generierung der kryptographischen Schlüssel festlegt. Die einzuleitenden Massnahmen sind

aber nicht beschrieben, wenn die bestehenden Schlüssel der Zertifizierungsstelle den möglichen neuen Anforderungen nicht mehr genügen und die Zertifizierungsstelle selber für den Eigengebrauch (Ausstellung der Zertifikate) einen neuen Schlüssel generieren muss (vgl. auch zu Art. 11). Der Wechsel des Signierschlüssels der Zertifizierungsstelle ist nicht geregelt. Also fehlt es auch an einem gesetzlich vorgeschriebenen Notfallkonzept.
Weiter fehlt es an Regelungen und gesetzlichen Aussagen bezüglich der Rechtsgültigkeit und der Aufbewahrungsvorschriften bestehender Rechtsabschlüsse, wenn der Signierschlüssel einer Partei kompromittiert worden ist.

SAV Un autre point essentiel pour assurer la sécurité de la signature électronique, est la possibilité de déterminer de façon sûre le moment de son utilisation.
Ein handelsübliches Computersystem lässt sich zurückdatieren. Zu Problemen führt dieser Umstand, wenn zwar ein Zertifikat widerrufen wird, es aber einer Drittperson gelingt, eine Rückdatierung vorzunehmen in eine Zeit der noch bestehenden Gültigkeit. In einer solchen Situation wirkt sich die Beweislastumkehr von Art. 17 zuungunsten des Zertifikatsinhabers aus. Aus diesem Grund stellt sich zumindest die Frage, ob es richtig ist, den Aspekt der Zeitstempel als „weiteren Dienst" von Zertifikatsanbietern ausserhalb des Geltungsbereichs des neuen Bundesgesetzes „anzusiedeln".
L'ajout automatique de l'indication du moment de l'utilisation de la signature électronique serait de nature à augmenter la sécurité juridique de documents transmis par voie électronique par rapport aux documents transmis par voie traditionnelle.

SBV Nous proposons de biffer l'al. 2 de l'art. 7. Nous vous renvoyons pour le surplus à notre commentaire relatif à l'art. 23.

SWICO Dieser Artikel ist viel zu wenig detailliert und Bedarf dringend der Ergänzung. Es sind die wichtigsten Verfahren und Mindestanforderungen zu beschreiben (vgl. EU Richtlinie, Anhang III). Abs. 1 soll (zwecks Verweis auf Art. 23) lauten: „*Der Bundesrat regelt in den Ausführungsvorschriften die Generierung kryptografischer Schlüssel, ...".*
Abs. 2 kann ersatzlos gestrichen werden, ist doch eben derselbe Satz auch in Art. 23 enthalten und dort wohl auch richtig platziert.

321.08 Art. 8

Kantone / Cantons / Cantoni

AG Gemäss Art. 1 bezweckt das BGES die Förderung eines breiten Angebotes an sicheren Diensten der elektronischen Zertifizierung. Ausgehend von diesem Zweckgedanken ist aus Sicht des Datenschutzes nicht nur die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift von Relevanz, sondern auch (oder gerade) die hierbei zugrundeliegende Technologie und insbesondere deren Förderung. Der Einsatz und die Verbreitung der Kryptographie sind wichtige Postulate des Datenschutzes. Dank kryptographischen Verfahren kann für die elektronische Datenkommunikation nicht nur Verbindlichkeit, sondern auch Vertraulichkeit, Integrität und Authentizität gewährleistet werden. Die Kryptographie unterstützt zentrale Anliegen des Datenschutzes und der Datensicherheit.

BL Wir schlagen vor, Art. 8 des Gesetzesentwurfs mit einem Absatz zu ergänzen, wonach auf Antrag des Gesuchstellers an Stelle seines offiziellen Namens ein Pseudonym vergeben werden kann, das nur auf Antrag veröffentlicht wird. Damit kann verhindert werden, dass anhand der Signatur ein persönliches Profil des Gesuchstellers erstellt werden kann. Selbstverständlich muss einem Unter-

suchungsrichter aber trotzdem möglich sein zu erfahren, wem ein solcher „pseudonymer“ Schlüssel zuzuordnen ist.

SG Wir beantragen, Art. 8 Abs. 1 Bst. b wie folgt zu formulieren: „den Hinweis, dass es in Anwendung dieses Gesetzes und *seiner* Ausführungsvorschriften ausgestellt wurde;“
Begründung: Angleichung der Formulierung an Art. 4 Abs. 1 Bst. f.
Vgl. auch zu Art. 9 / Cf. également ad art. 9 / Cf. anche ad art. 9.

TI A nostro parere il progetto dovrebbe comprendere anche le firme elettroniche delle persone giuridiche. Il sistema proposto, che prevede il rilascio di certificati elettronici solo alle persone fisiche (art. 8), non si applica infatti alle persone giuridiche, per le quali vale di regola il diritto di firma collettivo. Un documento elettronico emanante da una persona giuridica richiederebbe pertanto l'emissione di più certificati elettronici intestati ai diversi titolari del diritto di firma.

VD La loi allemande permet un champ d'information qui porte sur les limites de l'usage de la signature (par exemple mesure d'interdiction). Il semble encore que cette loi exige un champ qui spécifie l'algorithme utilisé, afin de disposer d'une donnée importante dans un contexte de technologie changeante.

Parteien / Partis / Partiti

Jungfreisinnige Gemäss Gesetz, können einzig natürliche Personen Inhaber einer digitalen Signatur sein. Wir können verstehen, dass es nicht einfach wäre, die Identität einer juristischen Person zu überprüfen. Wir verstehen auch die Problematik, die unter Artikel 3 des Begleitberichts zum Entwurf hervorgehoben wird. Trotzdem haben wir das Gefühl, dass vor allem Geschäftsbeziehungen zwischen Firmen einen Bedarf auf anerkannte digitale Signaturen haben. In dieser Hinsicht, fragen wir uns, ob es nicht sinnvoll wäre, eine Firmenunterschrift zu ermöglichen.
Erweiterung des Einsatzgebietes der digitalen Signatur auf die juristischen Personen, mit einem sogenannten Corperate-Key. Dabei werden die persönlichen digitalen Signaturen mit der Firmenbezeichnung erweitert.
Die Firma Swisskey vertreibt schon seit einiger Zeit diese Variante von digitaler Signatur. Sie basiert zwar auf einer persönlichen Unterschrift, enthält aber auch Informationen über die Firma, in der der Unterzeichnete arbeitet. Dadurch könnten auch die Probleme der Unterschriftsberechtigung von Angestellten transparenter gehalten werden. Der Lieferant oder Empfänger hat somit die Sigcherheit, dass der Angestellte unterschriftsberechtigt ist, und dieser auch in der Firma arbeitet, mit dem die Geschäftsbeziehung eingegangen wird.

PLS Il paraît indispensable de prévoir de manière exhaustive dans la loi les limites à l’utilisation du certificat. Les spécifications techniques nécessaires à un contrôle automatisé de ces limites devraient être définies dans l’ordonnance d’exécution. L’absence de telles limites, contrôlables automatiquement, risquerait de représenter une entrave majeure à la diffusion des certificats dans l’économie.

Organisationen / Organisations / Organizzazioni

CP Il nous paraît logique que la signature électronique ne puisse être attribuée qu'à des personnes physiques. En effet, les personnes morales ne peuvent, en droit suisse, s'engager juridiquement que par l'intermédiaire d'une personne physique.

economiesuisse Einzelne unserer Mitglieder bedauern, dass juristische Personen keine elektronische Unterschrift registrieren können, sondern nur natürliche Personen. Zwar ist anzuerkennen, dass auch nach geltendem Recht letztlich natürliche Personen eine juristische Person verpflichten. Die Registrierung von

elektronischen Unterschriften für juristische Personen würde jedoch weitgehende zusätzliche Fragen aufwerfen, und wir erachten es daher als richtig, heute und im Sinne einer raschen Inkraftsetzung auf diese Möglichkeit zu verzichten.

Damit digitale Signaturen über das Gültigkeitsdatum bzw. das Revozierungsdatum des zugehörigen Zertifikates hinaus gültig bleiben, müssen sie vorher, d.h. namentlich bei ihrer Erstellung, mit einem digitalen Zeitstempel versehen werden. Ohne Zeitstempel ist eine längere Aufbewahrung von ursprünglich gültigen digitalen Signaturen weitgehend nutzlos, da sie ihre Gültigkeit von selbst über die Zeit verlieren. Allerdings sehen andere unserer Experten darin ein technisches Detail, welches gesetzlich nicht vorgeschrieben werden muss, zumal Zertifikate üblicherweise terminiert sind. Das Verbot einer rückwirkenden Ausstellung von Zertifikaten ist selbstverständlich. Im Sinne einer klaren Definition regen wir unter diesem Artikel die Aufführung des Zeitstempels in einem elektronischen Zertifikat sowie eine Ergänzung unter Art. 3 an:

Zeitstempel: Eine mit einer digitalen Signatur versehene digitale Bescheinigung einer Anbieterin von Zertifizierungsdiensten, dass ihr bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben.

In der Botschaft ist darauf hinzuweisen, dass die „möglichen Nutzungsbeschränkungen“ gemäss Abs. 1 lit. c in den Ausführungsvorschriften spezifiziert und (z.B. analog der handelsrechtlichen Vollmacht) standardisiert werden müssen. Eine Erkennung bzw. Überprüfung solcher Nutzungsbeschränkungen muss maschinell möglich sein, andernfalls solche Zertifikate wegen des zu grossen Aufwandes im wirtschaftlichen Verkehr kaum akzeptiert werden könnten.

FGSec Abs. 1 Bst. b bedeutet, dass jedes Zertifikat auf das BGES verweist. Dies ist nicht kompatibel zur EU-Direktive, welche eine Referenz des „Qualifiziertes Zertifikat (Qualified Certificate)” verlangt. Es wäre angemessener, *„Swiss qualified certificate issued by an accredited certificate service provider”* als Referenz zu verwenden.

Bst. c sollte lauten: „Nutzungs- und/oder *Haftungs*beschränkungen.“

Der Name nach Bst. d muss ein „Distinguished name sein„ d.h. er muss eindeutig sein.

FHZ Es ist sicherzustellen, dass jede natürliche oder juristische Person einfach zu einem nach Schweizer Recht anerkannten Zertifikat kommen kann und auch durch das notwendige Handling nicht überfordert ist. Es ist zu überdenken, ob für die CA's ein Kontrahierungszwang besteht, dies vor allem für den Fall, dass nur wenige, ev. nur ein CA in der Schweiz besteht.

Einem ausländischen CA wird kein Kontrahierungszwang aufgelegt werden können. Es ist deshalb zu überdenken, für den Fall, dass es in der Schweiz keinen CA gibt, der Staat in die Lücke springen muss. Wie auch technisch vorgesehen, sind in lit. c) nicht Nutzungsbeschränkungen, sondern abschliessende positive Formulierungen der zulässigen Nutzung aufzuzählen.

Jeune Barreau vaudois Un problème se pose: la durée de validité d'un certificat électronique est limitée et peut être révoquée en tout temps. Se pose alors la question de la date de la signature du document informatique.

En effet, pour que la signature électronique sur un certificat valable puisse être assimilée à une signature manuscrite au sens du projet d'article 15a nouveau du code des obligations, il faudrait qu'elle soit accompagnée d'une mention de la date attestant du moment auquel la signature est intervenue. En l'absence

d'une telle indication, le signataire pourrait en effet prétendre que la signature est intervenue ultérieurement à la révocation du certificat.

KPMG Wir sind der Meinung, dass die möglichen Nutzungsbeschränkungen gemäss Art. 8 Abs. 1 präziser umschrieben und europakonform ausgestaltet werden sollten.

Das Zertifikat kann einen Hinweis auf mögliche Nutzungsbeschränkungen enthalten (Art. 8 Abs. 1 Bst. c). Als Beispiel einer solchen Nutzungsbeschränkung führt der Bericht die Kollektiv-Prokura (siehe Bericht, Seite 18) auf. Die Signaturrichtlinie sieht demgegenüber in Anhang I (Anforderungen an qualifizierte Zertifikate) drei verschiedene Nutzungsbeschränkungen vor:

- Beschränkungen des Geltungsbereichs des Zertifikats (Bst. i)
- Begrenzungen des Wertes der Transaktionen, für die das Zertifikat verwendet werden kann (Bst. j)
- Attribut des Unterzeichneten (Bst. d).
- Ob unter diese Art der Nutzungsbeschränkung auch eine Begrenzung des Wertes der Transaktionen, für die das Zertifikat verwendet werden kann (dies sieht bspw. Anhang I, Bst. j der RL EG 1999/93 vom 19.1.2000; Abl. Nr. L 13/12, vor), fällt, sagen weder das E-BGES noch der entsprechende Bericht. Hier braucht es, gerade wegen dieser europäischen Regelung, auch eine Aussage des schweizerischen Gesetzgebers. Schliesslich sollte aus unserer Sicht auch ein Vertretungsverhältnis über diesen Kanal kommuniziert und damit offengelegt werden können.

Unklar scheint uns demgegenüber die Bemerkung im Bericht (Seite 18), dass der Rechtsschein, den ein solches Zertifikat vermittelt, nicht taugt, die Vertretungsbefugnis zu verdrängen, wie sie sich aus dem Obligationenrecht und dem Handelsregister ergibt. Wir sind der Meinung, dass durch eine solche Nutzungsbeschränkung eine direkte Kundgabe an Dritte (ähnlich einer „externen Vollmacht“) im Sinne von Art. 33 Abs. 3 OR erfolgt und der Umfang der Vertretungsbefugnis sich demnach nach Massgabe der erfolgten Kundgebung richtet.

Muster/Sury Falls sich sehr viele Zertifizierungsdienste anbieten sollten, ist es ev. mit grossem Aufwand verbunden, zu überprüfen, ob das konkret eingesetzte Zertifikat tatsächlich von einer anerkannten Zertifizierungsstelle stammt und noch aktuell ist. Bei vielen CA's würde dieser Vorgang möglicherweise auch nicht mehr durch gängige Standardsoftware unterstützt werden. Die folgenden Ausführungen sollen den Hintergrund des Bedürfnisses der Möglichkeit der Einführung von Trustketten kurz ausführen.

Bevor mit der technischen Erläuterung begonnen werden kann, wird zuerst erklärt, was ein standardisiertes Zertifikat enthält. Es werden nur die Inhalte erwähnt, welche für das weitere Verständnis benötigt werden.

- Bezeichnung des Ausstellers
- öffentlicher Schlüssel des Ausstellers
- Bezeichnung des Nutzniessers
- öffentlicher Schlüssel des Nutzniessers
- Signatur, erstellt mit dem privaten Schlüssel des Austellers.

CA1 stellt dem Benutzer A ein Zertifikat Zert<A> aus. CA2 stellt dem Benutzer B ebenfalls ein Zertifikat Zert<B> aus. Benutzer A will nun mit dem Benutzer B einen Vertrag abschliessen und Waren im grösseren Wert bestellen. Benutzer B will nun zuerst das Zertifikat darauf verifizieren, ob es von einer anerkannten Zertifizierungsstelle erstellt worden ist. Ein Zertifikat kann primär jeder erstellen, weil die SW dazu auf dem Markt mehr oder weniger frei erhältlich ist. Also ist die Möglichkeit für einen Missbrauch gegeben. In einem Zertifikat steht zwar,

wer das Zertifikat ausgestellt hat, und der dazu passende öffentliche Schlüssel. B kann wohl nun anhand der Signatur des Zertifikats und anhand des im Zertifikat befindlichen öffentlichen Schlüssels die Signatur verifizieren, aber hat grundsätzlich keine Möglichkeit, zu prüfen, wer das Zertifikat ausgestellt hat.

B weiss also nicht, ob eine Konspiration von Benutzer A mit Benutzer C stattgefunden hat. C hat sich eine CA SW gekauft, stellt für Benutzer A Zertifikate aus und gibt sich dabei als eine anerkannte Zertifizierungsstelle CA1 aus. Weiter weiss B per se nicht, wo er die aktuelle Liste der von CA1 für ungültig erklärten Zertifikate beziehen kann.

Für die Lösung dieses Problems sind verschiedene Ansätze möglich. Hier drei Ansätze:

B lädt sich alle CA Zertifikate der anerkannten Zertifizierungsstellen in der Schweiz in seine Sicherheitsapplikation. Ein CA Zertifikat ist ein für sich selbst erstelltes Zertifikat einer Zertifizierungsstelle, wobei der Aussteller und der Nutzniesser des Zertifikats identisch sind. Folglich hat er eine Kopie des öffentlichen Schlüssels der CA1 geladen und kann diesen mit dem Inhalt des Rir A ausgestellten Zertifikats vergleichen. (Im Zertifikat ist der öffentliche Schlüssel des Ausstellers enthalten.) Die Lösung bringt den Nachteil der ständigen Aktualisierung der CA Zertifikate beim Benutzer B mit sich. Zudem muss der Ort der Ungültigkeitserklärung bekannt sein und aktualisiert werden.

CA1 und CA2 lassen sich gegenseitig ihre öffentlichen Schlüssel zertifizieren. CA1, rsp. CA2 stellt ein Zertifikat für den öffentlichen Schlüssel von CA2, rsp. CA1 aus. Diese werden publiziert. Nun kann Benutzer B im Verzeichnis von CA2 das von CA2 für CA1 erstellte Zertifikat lesen. Darin findet er eine „beglaubigte“ Kopie des öffentlichen Schlüssels. Anhand dessen kann er dann prüfen, ob dieser Schlüssel identisch mit dem Zertifikat von Benutzer A Zert<A> ist. Gleichzeitig könnte er im Zertifikat für CA1 den Ort des Verzeichnisses lesen, wo sämtliche von CA1 für ungültig erklärten Zertifikate abgelegt sind.

Es könnte aber auch eine staatliche Stelle die Zertifikate für die Zertifizierungsstellen anfertigen und publizieren.

Begriffe: Die gegenseitige Zertifizierung von öffentlichen Zertifizierungsschlüsseln bezeichnet man als Kreuzzertifikat. Eine Trustkette ist ein vollständiger und lückenloser Pfad von einer Zertifizierungsstelle zu einer anderen über CA Zertifikate.

Juristische Komplikation und Lösung

Die Kreuzzertifikate enthalten keine Bezeichnung einer natürlichen Person, sondern werden eher den Namen der Zertifizierungsstelle enthalten, was im allgemeinen der Name einer juristischen Person sein sollte.

Eine weitere Komplikation ergibt sich daraus, wann eine anerkannte Zertifizierungsstelle ein Zertifikat für eine andere Zertifizierungsstelle ausstellen kann und darf (Erlaubnis zum Erstellen von Kreuzzertifikaten). Vorschlag: Es darf ausschliesslich nur dann ein Kreuzzertifikat erstellt werden, wenn beide Zertifizierungsstellen rechtlich anerkannt worden sind.

Rosenthal Ein Zertifikat soll gemäss Art. 8 lediglich den Namen des Inhabers der Signatur enthalten, wobei unter dem Begriff des „Namens" im Sinne der Bestimmung vermutlich nur der bürgerliche Name einer Person (oder ggf. ein eindeutig zugeordnetes Pseudonym) gemeint ist.

Es ist fraglich, wie ein Zertifikat, das einzig auf „Peter Müller“ lautet (von denen im Schweizer Telefonbuch über 1'000 verzeichnet sind), auch nur annähernd zur sicheren Authentifikation, geschweige denn zu einer vernünftigen und effizienten Beweisbarkeit einer Willenserklärung führen kann.

Dass jeder dieser Peter Müller eine andere Seriennummer in seinem Zertifikat haben wird, ändert daran nichts. Zwar können anhand der Seriennummer durch Einsicht in die Akten des Zertifizierungsdienstanbieters womöglich weitere Personalien ermittelt werden, doch wäre dies aufwendig und damit nicht praxistauglich.

Ohnehin wäre der Zertifizierungsdienstanbieter nicht befugt, weitergehende Angaben über einen Zertifikatsinhaber zu liefern, die nicht schon aus dem Zertifikat ersichtlich sind. Soll ein Forderungsprozess durchgeführt werden, ist eine klare Personenidentifikation unerlässlich, und zwar noch bevor es zu einem Beweisverfahren kommt, da es keine schuldrechtliche Zivilklage gegen „Unbekannt“ gibt, in deren Verlaufe der wahre Beklagte ermittelt werden kann.

Wenn nicht klar ist, welcher Person ein Zertifikat bzw. eine Signatur zugeordnet werden kann, braucht ein Signatur-Inhaber im Streitfalle bloss zu behaupten, es handle sich um das Zertifikat eines Namensvetters. Umgekehrt könnte ein Signatur-Inhaber mit der eigenen Signatur, jedoch im Namen eines Namensvetters auftreten, ohne dass der Dritte Verdacht schöpfen würde und könnte.

Auch wenn anzunehmen ist, dass die Zertifizierungsdienstanbieter ihrerseits weitere Personalien zur Identifikation einer Person aufnehmen werden und dürfen, wäre es sinnvoll, wenn der Gesetzgeber seine Mindestanforderungen in diesem Punkt erweitert. Ansonsten wird er auch in einer Verordnung nicht kontrollieren und vorschreiben können, welche weiteren Personalien die Zertifizierungsdienstanbieter verwenden müssen. Die Zertifikate verschiedener Ausgabestellen wären nicht mehr unbedingt kompatibel.

Eine weitergehende Regelung wäre auch aus datenschutzrechtlicher Sicht erforderlich, um der Aufnahme weiterer Personendaten in die Zertifikate die nötige gesetzliche Grundlage zu verleihen, die eine Bearbeitung (insb. Nennung) auch gegen den Willen des Betroffenen möglich macht.

SBB Wir gehen davon aus, dass der Bundesrat der Zuordnung der Schlüssel zu einer juristischen Person sowie der Authentifizierung ihrer Willenserklärungen im Falle einer Doppelunterschriftsregelung in den geplanten Ausführungsvorschriften Rechnung tragen wird.

SBV Limites à l'utilisation du certificat (art. 8 al. 1 lit. c): Les limites éventuelles à l'utilisation du certificat devraient être énumérées de manière exhaustive dans la loi. Il ne s'agit pas seulement, en l'occurrence, de limites à l'utilisation du certificat, mais d'informations supplémentaires de nature à faciliter un traitement automatisé. Le destinataire de la signature devrait être tenu d'examiner ces indications. Les standards nécessaires existent déjà, de sorte qu'un tel système serait réalisable au plan technique.

Indications complémentaires (art. 8 al. 1 lit. g): Afin de faciliter la reconnaissance ultérieure des fournisseurs suisses de services de certification, les exigences de la loi devraient reprendre celles prévues dans l'annexe 1 à la directive européenne sur un cadre communautaire pour les signatures électroniques. Nous proposons, à tout le moins, de compléter l'art. 8 al. 1 lit. g comme suit:

„g. le nom et la signature numérique du fournisseur de services de certification qui le délivre ainsi que le pays dans lequel il est établi.“

„g. den Namen und die digitale Signatur der Anbieterin von Zertifizierungsdiensten, die es ausstellt sowie den Staat, in dem sie niedergelassen ist.“

Emission de certificats électroniques pour des personnes morales (art. 8 al. 1): L'art. 8 al. 1 stipule que les certificats électroniques délivrés au sens de la loi doivent être attribués à une personne physique. Conformément à la loi alle-

mande sur la signature électronique, le projet de loi exclut de la sorte l'émission de certificats pour des personnes morales.
La volonté des personnes morales s'exprime par leurs organes, c'est-à-dire par l'intermédiaire de personnes physiques ayant capacité de les engager. L'émission, pour une personne morale, d'une paire de clés cryptographiques propre, différente de celles des personnes physiques qui agissent habituellement en son nom, soulève des questions d'ordre juridique en particulier. Notre Association approuve dès lors, en l'état actuel, la solution retenue dans le projet de loi.

Schlauri/Kohlas Laut Art. 8 Abs. 1 Bst. d muss ein Zertifikat den Namen des Inhabers oder der Inhaberin des öffentlichen Prüfschlüssels enthalten.
Dies ist für eine eindeutige Identifikation dieser Person jedoch nicht ausreichend, denn sobald mehrere Personen denselben Namen tragen, können gezielt Verwechslungen herbeigeführt werden. Insbesondere könnte der Signierschlüsselinhaber unter Umständen sogar *abstreiten*, dass er überhaupt über ein Zertifikat verfügt, und behaupten, das eingesetzte Zertifikat sei von einer anderen Person gleichen Namens beantragt worden.
Um Verwechslungen zu verhindern, sind dem Zertifikat also zusätzliche Informationen hinzuzufügen, wie beispielsweise Nummer und Art des bei der Identifikation des Signierschlüsselinhabers eingesetzten amtlichen Dokumentes. Dabei muss darauf geachtet werden, dass auch Ausländer ein Zertifikat beantragen können.
Allfälligen aus diesen zusätzlichen Angaben erwachsenden Bedenken betreffend Datenschutz kann durch Einführung von Pseudonym-Zertifikaten Rechnung getragen werden.
Wir schlagen damit eine Änderung von Art. 8 Abs. 1 Bst. d vor (in Anlehnung an §7 Abs. 1 Ziff. 1 des neuen deutschen Signaturgesetzes vom 9. 3. 2001): *d. den Namen des Inhabers oder der Inhaberin des Prüfschlüssels, der im Falle einer Verwechslungsmöglichkeit mit einem unterscheidenden Zusatz zu versehen ist.*
Art. 8 Abs. 1 Bst. c VE-BGES sieht vor, dass in einem Zertifikat Nutzungsbeschränkungen vorgesehen werden können.
Die generelle Zulassung natürlichsprachlicher Nutzungsbeschränkungen könnte einerseits die automatische Auswertung von Zertifikaten beeinträchtigen und andererseits zu Auslegungsschwierigkeiten führen (dazu D. Rosenthal, Digitale Signaturen: Von Missverständnissen und gesetzlichen Tücken, Jusletter 29. Januar 2001, Rz 7). Aus diesen Gründen ist zu prüfen, ob nicht allenfalls ausschliesslich eine zahlenmässige Haftungslimite zugelassen werden soll.
In jedem Fall sollte in den technischen Ausführungsbestimmungen für eine zahlenmässige Haftungslimite zumindest ein standardisiertes Datenformat vorgesehen werden, das eine automatische Auswertung von Zertifikaten zulässt.
Sowohl der aktuelle Regelungsvorschlag als auch der Begleitbericht lassen offen, ob unter Nutzungsbeschränkungen auch Angaben über Vertretungsbefugnisse zu verstehen sind. Eine entsprechende Regelung, entweder durch zusätzliche Angaben im Zertifikat oder durch separate Attributzertifikate wäre u.E. sinnvoll und könnte etwa der Regelung von §7 Abs. 1 Ziff. 9 bzw. §7 Abs. 2 des neuen deutschen Signaturgesetzes entsprechen.

SIK Der Satz sollte u. E. offenbar heissen: die (zertifizierte) digitale Signatur *der Person, die* es *bei* der Anbieterin von Zertifizierungsdiensten ausstellt." Auch im französischen Text ist es irreführend (sollte nicht nur von uns bemerkt worden sein).

SVV Die Anpassungen der Bestimmungen zum Handelsregister sind grundsätzlich zu begrüssen. Bedauerlich ist der Umstand, dass die Verfasser des Vorentwurfs vom Konzept abgekommen sind, auch juristischen Personen den Zugang zu eigenen elektronischen Signaturen zu ermöglichen. Diese Idee lag zumindest noch der Zertifizierungsdiensteverordnung zu Grunde. Ohne weiteren Kommentar wird im Begleitbericht angefügt, dass sich dadurch nur schwer lösbare rechtliche Konflikte mit Eckwerten der geltenden Rechtsordnung ergäben. In Anbetracht der Möglichkeiten, welche die elektronische Signatur diesbezüglich eröffnen würde, wäre ein Überdenken dieser Position aus Sicht aller Anwender wünschenswert. Immerhin könnte das Handelsregisteramt selbst als Zertifizierungsdienstanbieter für Firmen auftreten, was die Prüfung der Zeichnungsberechtigung entscheidend vereinfachen und gleichzeitig eine potentielle neue Einnahmequelle erschliessen würde. Unter den gegebenen Umständen ist bei Firmenunterschriften nebst dem öffentlichen Schlüssel das Handelsregister stets noch separat zu prüfen.

SWICO Die EU-Richtlinie sieht auch Zertifikate z.G. von Juristischen Personen vor, womit sich die Frage stellt, ob es richtig ist, dass die Schweiz eine andere Lösung wählt. (i)aus der Sicht Klarheit, (ii)aus der Sicht, dass die digitale Signatur dem Gültigkeitserfordernis der einfachen Schriftlichkeit genügt, und (iii)aus der Sicht, dass die elektronische Signatur eigentlich nichts anderes als eine Alternative zum Schriftzug einer eigenhändigen Unterschrift sein soll, wäre die Schweizerlösung grundsätzlich systemkonform. Ebenso ist klar, dass in der Gleichstellung der digitalen Signatur mit der eigenhändigen Unterschrift (bzw. mit dem Zertifikat) nicht gleichzeitig auch eine „Vollmachtenregelung“ gesehen werden kann.

Auf der anderen Seite entspricht es einem Anliegen der Wirtschaft, wenn auch Zertifikate an Juristische Personen abgegeben werden könnten. Zudem würde dies die ganze Entpersonalisierung, die im elektronischen Rechtsverkehr rein faktisch besteht - denn hier kann nur das Legitimationsmittel und nicht auch der physische Mensch identifiziert werden -, letztlich nur unterstreichen. So ist denn auch die Juristische Person nur ein vom Gesetz künstlich geschaffenes Rechtsgebilde, welches letztlich immer nur durch besonders ermächtigte physische Personen handeln kann. Damit braucht jede physische Person, welche die Juristische Person vertritt, eine entsprechende Ermächtigung - sei es eine gesellschafts- bzw. handelsrechtliche oder eine gewillkürte. Damit wäre es für den Empfänger sehr praktisch und durchaus der Entpersonalisierung des elektronischen Geschäftsverkehrs entsprechend, wenn dieser das zusätzliche Erfordernis der Ermächtigung nicht auch noch prüfen müsste. - Ob jedoch die Juristischen Personen als Inhaber der elektronischen Signatur diesen zusätzlichen administrativen Aufwand bzw. das zusätzliche innerbetriebliche Missbrauchsrisiko übernehmen will, dürfte wohl kaum schlüssig beantwortet werden können.

Klar ist jedoch, dass nur Juristische Personen und nicht auch andere Gesellschaftsformen in den Genuss eines Zertifikatsinhabers kommen dürften. Die Einführung von Zertifikaten für Juristische Personen könnte sodann eine ganze Reihe von Anpassungen im Gesellschaftsrecht sowie im BGES als solches auslösen, was die Sache nicht vereinfacht und Zeit kosten wird.

Eine Expertenkommission hätte diese Fragen genauer beleuchten müssen. An dieser Stelle hat der Gesetzesentwurf wesentliche Auswirkungen auf die Kosten, die bei der Einführung dieser Technologie anfallen.

Abs. 1 lit. c ist u.E. aus praktischen Überlegungen heraus näher zu spezifizieren, und zwar indem die möglichen Nutzungsbeschränkungen abschliessend einzeln aufgezählt würden (wie dies z.B. auch bei der handelsrechtlichen, OR Art. 458 ff., Vollmacht getan ist). Dabei geht es nicht nur um Nutzungsbeschränkungen, sondern auch um Zusatzinformationen, die die automatische Verarbeitung erleichtern (vgl. die Ausführungen zu Art. 3, „Attribute"). Gleichzeitig muss dem Empfänger der Signatur die Pflicht auferlegt werden, diese Attribute zu prüfen. Technisch ist dies möglich, die notwendigen Standards existieren bereits heute.
Abs. 2 sollte (zwecks Verweis auf Art. 23) lauten: *„.. Der Bundesrat regelt das Format der Zertifikate in den Ausführungsvorschriften."*
Es fehlt ausserdem die Angabe des Niederlassungsstaates des Zertifizierungsdiensteanbieters (gemäss EU-Richtlinie, Anhang I).

TSM Im Begleitbericht (S. 16) ist festgehalten, dass nur natürliche Personen elektronisch signieren können. Diese Regelung leuchtet ein, da juristische Personen nur durch natürliche Personen handeln und auch nur diese persönlich unterschreiben können. Bezüglich der Unterschriftenregelung von Unternehmungen sollte man aber folgendes nicht vergessen: In vielen Betrieben dürfen die Mitarbeitenden (z.B. Prokuristen) nur kollektiv zu zweien unterschreiben. Die Möglichkeit einer solchen doppelten Unterschrift muss auch auf elektronischem Weg möglich sein, da sonst die Wirtschaft, als wichtige Betroffene der elektronischen Signatur, unberücksichtigt bleibt.

321.09 Art. 9

Gerichte / Tribunaux / Tribunali

BGr Nicht geregelt ist die (allfällige) Rechtsmittelordnung gegen die Entscheidungen der Anbieterinnen von elektronischen Zertifizierungsdiensten (Art. 9 ff.). Bestehen dagegen nur die aufsichtsrechtlichen Möglichkeiten gemäss Art. 15?

Kantone / Cantons / Cantoni

BS Aus dem Begleitbericht ergibt sich, dass auf die persönliche Vorweisung von Dokumenten vor der Anbieterin verzichtet werden kann, falls die persönliche Vorweisung von Dokumenten bei einer dritten Stelle erfolgt ist. Einmal muss die persönliche Vorweisung von Dokumenten erfolgen. In missverständlicher Weise erweckt Art. 9 Abs. 2 den Eindruck, dass auf sie ganz verzichtet werden kann.

NE L'identification des personnes qui demandent la délivrance d'un certificat électronique est extrêmement importante du moment où il s'agit de la première mesure de sécurité sur laquelle repose le système retenu. Cette identification doit se faire très soigneusement, puisque la loi proposée demande que ces personnes établissent leur identité en se présentant personnellement. Le Conseil fédéral admet que la procédure d'identification des requérants de certificats électroniques est une tâche qui peut être déléguée à des tiers qui ont qualité de bureau d'enregistrement. A titre d'exemple, il cite les bureaux de poste ou les succursales bancaires, lesquels pourraient fonctionner comme bureaux d'enregistrement, mais sans apporter une sécurité quelconque au processus d'identification. Or, ne serait-ce pas l'apanage même des notaires, dont le réseau est particulièrement dense sur l'ensemble du territoire, d'avoir la mission d'établir l'identité des personnes et, ainsi, de fonctionner comme bureaux d'enregistrement? Cette procédure serait pourtant la seule susceptible d'apporter à la vérification de l'identité des requérants de certificats électroniques la sécurité juridi-

que qu'une telle opération exige, notamment en raison de la force probante des actes authentiques (art. 9 CCS).

SG Zum Identitätsnachweis nach Art. 9 Abs. 1 sind nur Dokumente zuzulassen, die auf dem Zivilstandsregister basieren (z.B. Identitätskarte). Vom ausnahmsweisen Verzicht auf die persönliche Vorweisung von Dokumenten ist Abstand zu nehmen.
Begründung: Aufgrund der erhöhten Missbrauchsgefahr im elektronischen Geschäftsverkehr ist eine eindeutige Identifikation der natürlichen Person unerlässlich.

VD L'exigence selon laquelle les personnes à qui des certificats sont délivrés doivent se présenter en personne devant les fournisseurs de services laisse songeur puisque le projet de loi vise précisément à permettre de valider les actes juridiques entre personnes n'étant pas en contact physique.
Etant donné que la titularité d'une signature électronique est vraisemblablement appelée à devenir une condition sine qua non d'accès au commerce électronique et aux informations disponibles sur internet, il serait judicieux que les conditions de délivrance de cette signature ne soient pas trop restrictives ni prohibitives, notamment sur le plan financier.
En revanche, étant donné l'importance de l'identification initiale, la loi ou l'ordonnance devrait indiquer avec précision quels sont les documents probants. La référence à „certains documents“ est trop vague.

Parteien / Partis / Partiti

PLS L'ordonnance devrait définir clairement la nature des documents susceptibles d'être fournis au moment de l'identification. Pour les personnes physiques, il devrait s'agir d'une carte d'identité, d'un passeport ou d'un document officiel analogue. De plus, pour permettre un meilleur contrôle de la procédure d'identification, le fournisseur de services de certification devrait être tenu de conserver une copie des pièces présentée lors de l'identification.

Organisationen / Organisations / Organizzazioni

CP L'activité essentielle des fournisseurs de services de certification consiste à délivrer des certificats électroniques attestant qu'une clé publique est liée à une personne déterminée. L'identification des demandeurs doit donc être faite avec sérieux. La délégation de compétence telle que proposée ne fait que consacrer juridiquement la pratique. Nous en prenons donc acte.

economiesuisse Es muss klargestellt werden, welche Unterlagen im Zusammenhang mit dem Erhalt eines Zertifikates vorgelegt werden müssen. Diese Präzisierung kann auf Verordnungsebene erfolgen. Die notwendigen Identitätspapiere müssen die Verwendung der elektronischen Unterschrift etwa auch im Zusammenhang mit den Identifikationspflichten nach dem Geldwäschereigesetz gewährleisten. Entsprechend müsste die Vorlage eines Identifikationspapiers wie Identitätskarte, Pass oder eines ähnlichen amtlichen Dokumentes verlangt werden.
Es ist ein neuer Absatz gemäss folgendem Wortlaut aufzunehmen: Die anerkannten Anbieterinnen von Zertifizierungsdiensten können ihre Aufgabe zur Identifikation eines Zertifikatsantragstellers gemäss Abs. 1 an Dritte, sogenannte Registrierungsstellen, delegieren. Für die korrekte Ausführung der Aufgabe durch die Registrierungsstellen haftet jedoch allein die anerkannte Anbieterin von Zertifizierungsdiensten.
Diese Möglichkeit entspricht dem status quo und findet im Begleitbericht ausdrückliche Erwähnung. Angesichts ihres weitreichenden Einflusses auf die

Rechte und Pflichten der Zertifizierungsdienstanbieterinnen wie auch der Registrierungsstellen gehört diese Bestimmung aber in das Gesetz. Konsequenterweise muss diese Ergänzung an den notwendigen Stellen im Gesetz berücksichtigt werden (z.B. Art. 10 Abs. 3 oder Art. 14 Abs. 1).

Es sollte ferner geregelt werden, dass die anerkannten Anbieterinnen von Zertifizierungsdiensten keine Kopien der privaten Signaturschlüssel ihrer Kunden und Kundinnen aufbewahren dürfen.

EKK L'art. 9 du projet de loi prévoit des conditions relativement strictes à observer pour la délivrance des certificats électroniques. Ces exigences sont assurément à la hauteur de l'importance qui sera faite de ces certificats dans le domaine des relations commerciales électroniques. Elles ne pourront donc que contribuer à augmenter la confiance des consommateurs qui utiliseront la signature électronique à l'avenir.

Néanmoins, la Commission demande que le Conseil fédéral prévoie un réseau pratique de bureaux d'enregistrement pour que le consommateur puisse s'y rendre sans trop d'encombres pour s'y voir délivrer un certificat électronique.

FRC Wie / Comme / Come EKK.

FRI Les articles relatifs notamment à la délivrance et l'annulation des certificats électroniques décrivent avec pertinence les obligations des fournisseurs de services de certification. Il s'agira dès lors de faire respecter ce quasi „code de conduite" dont dépend la fiabilité du système tout entier.

kf Wir würden es vorziehen, wenn klar ausgedrückt steht, welche persönlichen Dokumente hier gemeint sind. Es ist deshalb auch unklar, wieso ein Abs. 2 überhaupt nötig ist.

Muster/Sury Eine anerkannte Zertifizierungsstelle müsste dazu verpflichtet sein, für alle die bei ihr um ein Zertifikat begehrenden Personen ein Zertifikat auszustellen, wenn nicht gewichtige Gründe dagegen sprechen. Ansonsten könnten gewisse juristische und natürliche Personen in ihrer wirtschaftlichen Freiheit eingeschränkt oder behindert werden.

SBV L'identification des personnes sollicitant un certificat électronique est une tâche essentielle du fournisseur de services de certification. Il nous paraît dès lors nécessaire de préciser, dans l'ordonnance, la nature des documents qui doivent être présentés lors de l'identification. Afin de satisfaire aux exigences de la législation sur le blanchiment d'argent, nous estimons qu'il doit s'agir, pour les personnes physiques, d'une carte d'identité ou d'un passeport.

Par ailleurs, afin que la vérification de l'identité puisse être contrôlée, nous sommes d'avis que le fournisseur de services de certification devrait être tenu de conserver une copie des documents (carte d'identité ou passeport) ayant servi à identifier la personne requérant le certificat. Cette exigence devrait figurer expressément dans l'ordonnance.

Délégation de l'identification à des tiers (art. 9 al. 2): Le commentaire relatif au projet de loi souligne que l'identification des requérants de certificats électroniques est „une tâche qui peut très bien être déléguée à des tiers (bureaux d'enregistrement)", étant précisé toutefois que le fournisseur de services de certification reconnu reste seul responsable de l'accomplissement correct de ses obligations par ces tiers. Afin d'éviter toute incertitude à ce sujet, nous proposons de stipuler expressément, dans la loi, la possibilité d'une telle délégation ainsi que la responsabilité qui en découle pour le fournisseur de services de certification. En cas d'acceptation de cette proposition, il y aurait lieu d'ajouter un al. 2 nouveau à l'art. 9 et d'adapter en conséquence plusieurs dispositions du projet de loi (en particulier les art. 10 al. 3 et 14 al. 1).

L'art. 9 al. 2 nouveau pourrait avoir la teneur suivante:
„Les fournisseurs de services de certification reconnus peuvent déléguer les tâches qu'ils exercent en relation avec l'identification d'une personne souhaitant obtenir un certificat électronique à des tiers (bureaux d'enregistrement). Ils sont cependant seuls responsables de l'exécution correcte de ces tâches par les bureaux d'enregistrement".
„Die anerkannten Anbieterinnen von Zertifizierungsdiensten können ihre Aufgabe zur Identifikation eines Zertifikatsantragstellers gemäss Abs. 1 an Dritte, sogenannte Registrierungsstellen, delegieren. Für die korrekte Ausführung der Aufgabe durch die Registrierungsstellen haftet jedoch allein die anerkannte Anbieterin von Zertifizierungsdiensten."
A toutes fins utiles, nous attirons l'attention sur le fait que la loi allemande révisée sur la signature électronique prévoit expressément la possibilité, pour le fournisseur de services de certification, de déléguer certaines tâches à des tiers (voir § 4 ch. 5 de cette loi).

SVV „Die anerkannten Anbieterinnen von Zertifizierungsdiensten müssen von den Personen, die einen Antrag auf Ausstellung eines elektronischen Zertifikats stellen, den Nachweis ihrer Identität durch persönliche Vorweisung bestimmter Dokumente verlangen. Sie müssen sich ferner vergewissern, dass die Person, die ein elektronisches Zertifikat verlangt, *spätestens im Zeitpunkt der Ausstellung* des Zertifikats im Besitz des entsprechenden privaten Signaturschlüssels ist."
Begründung: Der aktuelle Wortlaut von Art. 9 lässt darauf schliessen, dass die Person, die ein elektronisches Zertifikat verlangt, im Besitz des entsprechenden privaten Signaturschlüssels ist. Auch hier besteht zwar die theoretische Möglichkeit, dass der private Schlüssel durch den Ansprecher selber generiert werden kann. Im klassischen Fall wird die Person, die ein elektronisches Zertifikat verlangt, aber erst am Ende des Identifikationsprozesses im Besitze des privaten Schlüssels sein. Wir schlagen der Klarheit halber deswegen auch hier vor, die Formulierung breiter zu fassen. Danach hat sich der Anbieter spätestens im Zeitpunkt der Ausstellung des Zertifikates zu vergewissern, dass der Ansprecher im Besitz des privaten Signaturschlüssels ist.

SWICO Laut Erläuterungen soll die Zertifizierungsstelle Dritte zur Erfüllung ihrer Leistungen beiziehen dürfen - so etwa zwecks Identifikationsprüfung -, wobei die Zertifizierungsstelle uneingeschränkt für das Handeln des Dritten einzustehen hätte, wie wenn sie selber gehandelt hätte. Eben diese Sachlage wird bereits heute etwa von der Firma SWISSKEY z.B. mit Banken (sogenannte Registrierungsstellen) gelebt. Diese Sachlage ist u.E. im Gesetz unbedingt aufzunehmen und entsprechend zu regeln (Beizug von Dritten, inkl. Haftungsfolgen). Kommt der Gesetzgeber diesem Begehren nach, wäre an diversen anderen Orten des BGES auch eine entsprechende Ergänzung vorzunehmen (so etwa: Art. 10 Abs. 3, Art. 14).
Zwischen den bestehenden Absätzen könnte mit dem nachfolgenden Text (als zusätzlicher Absatz) dem vorstehenden Anliegen nachgekommen werden: *„Die anerkannten Anbieterinnen von Zertifizierungsdiensten können ihre Aufgabe zur Identifikation eines Zertifikatsantragstellers gemäss Abs. 1 an Dritte, sogenannte Registrierungsstellen, delegieren. Für die korrekte Ausführung der Aufgabe durch die Registrierungsstellen haftet jedoch allein die anerkannte Anbieterin von Zertifizierungsdiensten."*

321.10 Art. 10

Kantone / Cantons / Cantoni

AG Wenn Art. 10 - wie die aktuelle Zertifizierungsdiensteverordnung - einzig festhält, die Zertifizierungsdienste müssten ihre Kunden spätestens bei der Ausstellung der elektronischen Zertifikate auf die Folgen eines möglichen Missbrauchs oder Verlustes des privaten Schlüssels aufmerksam machen und sie müssten ihnen geeignete Massnahmen zur Geheimhaltung des privaten Schlüssels vorschlagen, zeigen sich die Probleme der praktischen Umsetzung in deutlicher Weise: Dem nach Art. 16 BGES umfassend in die Pflicht genommenen Kunden sind die Abläufe in seinem Informatikumfeld in aller Regel nicht bekannt. Eine geeignete Massnahme zur Geheimhaltung des privaten Schlüssels könnte somit etwa darin gesehen werden, dass dem Kunden Komponenten (PC, Tastatur und Kartenleser) zur Verfügung gestellt würden, für die eine vertrauenswürdige Stelle - in der Regel wohl eine staatlich anerkannte Stelle - bestätigt, dass diese sicher arbeiten, insbesondere den privaten Schlüssel nicht kopieren.

AR Im selben Sinne wie / Dans le même sens que / Nello stesso senso di ZH.

BL Art. 10 hält wie die geltende Zertifizierungsdiensteverordnung lediglich fest, die Zertifizierungsdienste müssten ihre Kunden spätestens bei der Ausstellung der elektronischen Zertifikate auf die Folgen eines möglichen Missbrauchs oder Verlusts des privaten Schlüssels aufmerksam machen und ihnen geeignete Schutzmassnahmen vorschlagen. Die praktische Umsetzung dieser Vorschrift wird allerdings Probleme bereiten: Dem nach Art. 16 des Entwurfs umfassend in die Pflicht genommenen Kunden sind die Abläufe in seinem Informatikumfeld in aller Regel völlig undurchschaubar. Eine geeignete Massnahme zur Geheimhaltung des privaten Schlüssels könnte etwa darin gesehen werden, dass dem Kunden Komponenten (PC, Tastatur und Kartenleser) zur Verfügung gestellt würden, für die eine vertrauenswürdige Stelle – in der Regel wohl eine staatlich anerkannte Stelle – bestätigt, dass diese sicher arbeiten, insbesondere den privaten Schlüssel nicht kopieren. Da es solche Komponenten zur Zeit nicht gibt, fehlt es auch an staatlich anerkannten Bestätigungen. Ein verantwortungsbewusster Kunde wird – nicht zuletzt wegen der Beweislastumkehr bei Missbrauch gemäss Art. 17 des Entwurfs – von den ihm im Gesetz vorgeschlagenen Zertifikaten keinen Gebrauch machen. Die heute schon auch ohne gesetzliche Anerkennung zur Verfügung stehenden Zertifikate werden ihm bessere Dienste leisten.

Für die Kantone bedeutet dies, dass sie zur Einführung von E-Government in ihren Erlassen – beispielsweise zur Gültigkeit einer elektronischen Eingabe, aber auch für den elektronischen Informationsaustausch zwischen Behörden und Bürgern – nicht auf die Lösung des Bundesgesetzes über die elektronische Signatur zurückverweisen dürfen. Die vom Bundesgesetz ausgehenden Impulse bestehen daher in erster Linie in der grundsätzlichen Anerkennung der eingesetzten Technologie und allenfalls in einer späteren Phase in den durch Bundesrats- oder Departementsverordnungen festgelegten technischen Regelungen.

FR Wie / Comme / Come BL.

GL Im selben Sinne wie / Dans le même sens que / Nello stesso senso di ZH.

GR Ob sich die digitale Signatur im Rechtsverkehr durchsetzt, wird entscheidend davon abhängen, inwieweit sich die Vertragspartner auf sie verlassen dürfen. Der Haftungsregelung kommt in diesem Zusammenhang eine grosse Bedeu-

tung zu. Die Haftungsregeln im Entwurf (Art. 16-19) sind an sich sachgerecht. Trotzdem sind Probleme im Hinblick auf die Rechtsanwendung erkennbar.
Wenn im erläuternden Bericht zu Art. 16 bezüglich der Frage, welches Sorgfaltsmass die Inhaberinnen privater Signaturschlüssel bei der Aufbewahrung anwenden müssen, ausgeführt wird, niemand sei gehalten, für die Geheimhaltung seines privaten Signaturschlüssels sein Leben zu riskieren, so wird doch eine gewisse Hilflosigkeit im Hinblick auf die praktische Umsetzung deutlich. Es ist deshalb zu wünschen, dass in Ausführungsvorschriften konkretisiert wird, welches „geeignete Massnahmen zur Geheimhaltung des privaten Signaturschlüssels“ sind, die die anerkannten Anbieterinnen von Zertifizierungsdiensten ihren Kunden und Kundinnen gemäss Art. 10 Abs. 2 vorschlagen müssen. Aufgrund der technischen Entwicklung kann eine solche Konkretisierung allerdings nur beispielhaft und in genereller Form erfolgen. Immerhin würde damit die Rechtssicherheit für die Kundinnen und Kunden doch verbessert.

JU S'agissant de l'al. 3, il convient de relever qu'en vertu du renversement du fardeau de la preuve, la conservation des documents s'opère principalement en faveur des fournisseurs de services de certification puisqu'il appartient à ces derniers d'apporter la preuve qu'ils ont respecté leurs obligations (art. 18, al. 2).

TI Allo stadio attuale della tecnica nessun prestatore di servizi di certificazione può garantire una sicurezza totale ed escludere la possibilità di alterazioni o manipolazioni della chiave elettronica e perfino dell'integrità del testo trasmesso. Il prestatore di servizi di certificazione deve quindi informare in modo completo e trasparente gli utenti sui rischi insiti nell'uso di chiavi elettroniche e sulle responsabilità che gli incombono in caso di guasti tecnici (sovraccarico di linee, interruzioni di corrente, ecc.).
Per quel che concerne l'obbligo di archiviazione dei dati del prestatore di servizi di certificazione (art. 10 cpv. 3), la durata di conservazione deve essere armonizzata con le necessità degli uffici dei registri fondiari, i quali devono conservare a tempo indefinito i documenti giustificativi delle iscrizioni.

VD Compte tenu des dommages que pourrait entraîner un accès indu à la base publique du certificateur, la loi pourrait prévoir une obligation du certificateur d'informer le public, par l'intermédiaire de l'organisme d'accréditation, des pénétrations du système non autorisées.
Par ailleurs, de manière à faciliter l'administration des preuves, on pourrait prévoir une obligation d'information par écrit, à l'al. 2.

ZG Im selben Sinne wie / Dans le même sens que / Nello stesso senso di ZH.

ZH Nach Art. 16 Abs. 2 haben die Inhaberinnen und Inhaber privater Signaturschlüssel diese so aufzubewahren, dass ihre Verwendung durch unbefugte Dritte ausgeschlossen werden kann. Nach Art. 17 Abs. 2 haftet die Inhaberin oder der Inhaber für Schäden, die ein Dritter erleidet, weil er sich auf das gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten verlassen hat. Im Schadensfall wird die Einwilligung der Inhaberin oder des Inhabers zum Einsatz ihres Schlüssels vermutet. Ihnen obliegt es nach Art. 17 Abs. 1 zu beweisen, dass der Schlüssel ohne ihren Willen verwendet wurde. Die Folgen der Beweislosigkeit haben diesbezüglich also die Inhaberin oder der Inhaber des privaten digitalen Signaturschlüssels zu tragen.
Die digitale Signatur umfasst technisch hoch entwickelte und komplexe Abläufe und Verfahren (Art. 7 Abs. 1 letzter Satz verpflichtet den Bundesrat ausdrücklich für ein der technischen Entwicklung entsprechendes hohes Sicherheitsniveau zu sorgen). Transparenz und Kontrolle stellen in diesem Umfeld

hohe Anforderungen an die Beteiligten. Mit der Verpflichtung, die erforderlichen Vorkehrungen zu treffen, welche die Verwendung ihres digitalen Signaturschlüssels durch unbefugte Dritte ausschliessen, sind die Inhaberinnen und Inhaber der Schlüssel daher schnell überfordert. Der Gesetzesentwurf sieht deshalb - wie bereits die Verordnung über Dienste der elektronischen Zertifizierung vom 12. April 2000 (Art. 9) - in Art. 10 Abs. 2 vor, dass anerkannte Anbieterinnen von Zertifizierungsdiensten ihre Kundinnen und Kunden bei der Ausstellung der elektronischen Zertifikate auf die Folgen eines möglichen Missbrauchs oder Verlusts des privaten Signaturschlüssels aufmerksam machen und ihnen geeignete Massnahmen zur Geheimhaltung der privaten Signaturschlüssel vorschlagen müssen. Trotz dieser Regelung stellt die mit Art. 17 Abs. 1 vorgeschlagene Verteilung der Beweislast die technisch unerfahrenen Betroffenen im Haftungsfall vor erhebliche Beweisprobleme. Es fragt sich daher, ob die Instruktionspflicht der anerkannten Anbieterinnen von Zertifizierungsdiensten nach Art. 10 Abs. 2 als Mittel zur Vorkehr gegen die strenge Haftung der Inhaberinnen und Inhaber der digitalen Signaturschlüssel ausreicht. Besser wäre wohl, den Betroffenen über die Regelung von Art. 10 Abs. 2 hinaus auch konkrete Instrumente zur Geheimhaltung des privaten Schlüssels anzubieten (etwa PC, Tastatur und Kartenleser), deren sichere Arbeitsweise von einer vertrauenswürdigen Stelle bestätigt würde. Zurzeit stehen freilich weder solche Instrumente noch entsprechende Bestätigungsstellen zur Verfügung. Mit dieser Ausgangslage könnte aber die strenge Haftungsregelung des Gesetzesentwurfs dazu führen, dass nicht die vom Gesetz geregelten, sondern die heute bereits ohne gesetzliche Regelung zur Verfügung stehenden Zertifikate bevorzugt werden. Ohne die angeregte Erweiterung. werden die Kantone in ihren Erlassen zur Einführung von Electronic Government wohl nur in geringem Masse auf die Regelung des BGES verweisen können, im Übrigen aber eigene Bestimmungen erlassen müssen.

Organisationen / Organisations / Organizzazioni

CP Les fournisseurs de services de certification devront tenir à disposition du public leurs conditions générales. Les règles commerciales normales s'appliquent ici.

economiesuisse Es ist gerechtfertigt, dass die privaten Nutzer nachhaltig auf die Konsequenzen aufmerksam gemacht werden, welche sich im Zusammenhang mit ihrem privaten Signaturschlüssel ergeben können. An sich wäre es wünschbar, die gemäss Art. 10 Abs. 2 geforderten „geeigneten Massnahmen“, wenn nicht im Gesetz (was wegen der trägen Anpassbarkeit kaum realistisch ist), so doch in der Verordnung zu präzisieren. Im Gesetz selbst wäre Abs. 2 wie folgt zu ergänzen: „*...ihnen den Anforderungen der Ausführungsvorschriften genügende Massnahmen zur Geheimhaltung...“.*

FGSec Das Problem eines korrumpierten Terminals wird im BGES ignoriert. Dieses Problem stellt (neben der Verständnisfrage bei den Nutzern) das grösste Hindernis einer verbreiteten Verwendung dar.

Der Begleitbericht impliziert in 23, bzw. 231, dass ein E-Mail-Client eine akzeptable sichere Signaturerstellungseinheit ist. Wir sind der Überzeugung, dass diese Annahme falsch ist und dass E-Mail-Clients ein hohes Gefährdungspotential aufweisen.

Die Qualität der Benutzerschnittstelle (Human-Computer-Interface HCI) der sicheren Signaturerstellungeinheit muss ebenfalls behandelt werden. Sie muss die unbeabsichtigte Unterzeichnung verhindern, da diese zu rechtlichen Verbindlichkeiten führt.

Wir empfehlen, dass das BAKOM eine Richtlinie herausgibt, wie ein Nutzer seinen privaten Schlüssel aufbewahren, verwenden und schützen muss.
Diese Richtlinie muss dem Nutzer durch den CSP übergeben und bestimmt, wie sicher die Signaturerstellungseinheit sein muss und wie er dies gewährleisten kann.
Es ist möglich und problematisch, dass diese Richtlinie während der Lebensdauer eines Zertifikates nachgeführt und überarbeitet werden muss.
Der Name nach Bst. d muss ein „Distinguished name“ sein, d.h. er muss eindeutig sein.
Abs. 2 kann nur umgesetzt werden, wenn das BAKOM einen Standard-Text für die CSPs entwirft, welche diese an ihre Kunden weitergeben können. Der Text wird häufige Nachführungen aufgrund der fortschreitenden technologischen Entwicklung und der Bedrohung durch Unterwanderung verlangen.

FRC A rajouter: *„Le ou la cliente doit confirmer qu'elle a pris connaissance des conditions générales du contrat. Sans cette confirmation, le contrat n'est pas valable. De plus, pour des raisons de preuve, le consommateur est tenu de les imprimer“.*
Nous considérons qu'il s'agit là d'une mesure de précaution élémentaire. Les conditions générales sur Internet sont souvent rédigées en tout petits caractères et bien „cachées“. De même, il est nécessaire de les imprimer car les conditions générales peuvent changer et si elles n'ont pas été imprimées au moment de la conclusion du contrat, le consommateur peut subir de gros préjudices.
A rajouter: *„Le ou la cliente doit confirmer qu'il a été mis au courant des conséquences de la divulgation ou de la perte de sa clé privée et qu'il a pris connaissance des mesures que le fournisseur de services de certification lui a fournies pour maintenir sa clé privée secrète. En l'absence de confirmation, le contrat n'est pas valable"*.
La méconnaissance des risques techniques liés à Internet nécessite cette adjonction.

ISACA La loi délègue aux fournisseurs (CA) le soin de définir les „mesures appropriées„ qui pourront donc différer d’un fournisseur à l’autre. Cette notion, équivalente aux „mesures qu’exigent les circonstances“ de l’article 16, jouera un rôle essentiel, notamment dans la délimitation de la responsabilité du titulaire de la clé privée en cas de dommage à un tiers. Des mesures appropriées minimales devraient être définies de manière contraignante par le Conseil fédéral en application de l'art. 23.

kf Ergänzung: *„Die Kundin oder der Kunde muss jedes Mal durch „Quickwrapping“ bestätigen, von den allgemeinen Vertragsbedingungen oder den Folgen des Missbrauches oder Verlustes Kenntnis genommen zu haben. Nur dann kann er einen Schritt weiter gehen in der Vertragsabwicklung.“*
Oft sind die AGV auf Internet-Seiten schwer auffindbar, nicht ausdruckbar oder fehlen ganz. Mit dieser einfachen technischen Lösung können sich auch die Anbieter gegen unberechtigte Forderungen seitens der Kunden absichern und gleichzeitig wird klar ausgedrückt, wie wichtig die Kenntnisnahme dieser Vertragsbestimmungen sind.

SAV La distinction entre une signature valable au sens de la LFSél et une signature certifiée en apparence comme une signature valable, mais en réalité dépourvue de validité juridique au sens de la LFSél doit être évidente pour tout un chacun. Le degré de sécurité suffisant ne peut être atteint :

1. que s'il est interdit aux fournisseurs de services de certification de faire état de leur qualité de fournisseurs reconnus pour promouvoir aussi l'offre de certificats non conformes à ceux de la LFSél et,
2. que si l'obligation leur est faite d'indiquer expressément sur les certificats non conformes qu'ils ne valent pas comme signature au sens du droit suisse.

   Un simple renvoi aux conditions générales du fournisseur de services de certification n'offre aucune protection réaliste pour un utilisateur ordinaire.

A titre de sanction pour d'éventuelles violations, il serait souhaitable de prévoir dans la LFSél que, outre d'éventuelles sanctions administratives, les fournisseurs de services de certification (et pas seulement les fournisseurs reconnus) répondent des dommages qui résultent des confusions qui pourraient exister en Suisse entre les certificats valant signatures au sens de la LFSél et ceux qui n'ont pas cette portée.

SBV Aux termes du rapport explicatif, „l'activité essentielle des fournisseurs de services de certification consiste à délivrer des certificats électroniques attestant qu'une clé publique est liée à une personne ou à une entité administrative déterminée". Les activités se rapportant à l'émission de clés privées et publiques ne sont donc pas, en principe, du ressort des fournisseurs de services de certification. Dans ces conditions, il peut paraître problématique d'imposer à ces mêmes fournisseurs l'obligation d'informer leurs clients sur les mesures à prendre pour tenir leur clé privée secrète. Cela d'autant plus que de telles indications ont une incidence déterminante sur la responsabilité découlant d'une utilisation abusive de la clé privée.
En vue de faciliter l'obligation d'informer à la charge des fournisseurs de services de certification, il y aurait lieu à tout le moins de définir, dans l'ordonnance ou dans les prescriptions techniques, ce qu'il faut entendre par „mesures appropriées" au sens de l'al. 2. A cet effet, nous proposons de modifier l'art. 10 al. 2 dans le sens suivant: *„…ihnen den Anforderungen der Verordnung und der Ausführungsvorschriften genügende Massnahmen zur Geheimhaltung…" „….leur indiquer les mesures satisfaisant aux exigences de l'ordonnance et des prescriptions d'exécution pour maintenir…"*.

SVV Zu Abs. 2: Die Bestimmung verlangt, dass die anerkannten Anbieterinnen von Zertifizierungsdiensten ihren Kunden geeignete Massnahmen zur Geheimhaltung des privaten Signaturschlüssels vorschlagen. Die Bedeutsamkeit dieser Regel ergibt sich im Zusammenhang mit den Haftungsbestimmungen. So verlangt Art. 16 Abs. 2, dass die Inhaber privater Signaturschlüssel alle „nach den Umständen zumutbaren Vorkehrungen" zu treffen haben, damit eine Verwendung durch unbefugte Dritte ausgeschlossen werden kann.
Anders als die persönliche Unterschrift ist die elektronische Signatur leicht übertragbar. Dadurch eröffnen sich einerseits Chancen, andererseits aber auch Missbrauchsmöglichkeiten. Die Einhaltung der Geheimhaltungspflichten sind folglich von eminenter Wichtigkeit, nicht zuletzt weil Anbieter von Waren und Dienstleistungen im Internet davon ausgehen können müssen, dass sie auch tatsächlich mit dem Inhaber der Signatur verhandeln.
Werden die Ratschläge geeigneter Massnahmen den einzelnen Anbieter überlassen, besteht die Gefahr, dass je nach Anbieter unterschiedliche Anforderungen gestellt werden. Unklar ist überdies die Haftung, sollten Massnahmen empfohlen werden, die sich im Nachhinein als ungeeignet erweisen. Aus

Gründen der Rechtssicherheit beantragen wir deshalb, dass die Richtlinien durch den Bundesrat in der Vollzugsverordnung erlassen werden.
Abs. 3: Antrag: „Sie führen ein Tätigkeitsjournal. *Dieses ist zusammen mit den dazu gehörenden Belegen während 10 Jahren aufzubewahren.“*
In Abs. 3 wird eine bundesrätliche Kompetenz zu Ausführungsbestimmungen hinsichtlich der Aufbewahrung der Tätigkeitsjournale und der damit zusammenhängenden Belege statuiert. Die absolute Verjährungsfrist von Ansprüchen nach BGES beträgt nach Art. 19 zehn Jahre. Auch Art. 962 OR verlangt in Anlehnung an die Verjährungsfristen im Obligationenrecht für die Aufbewahrung der Geschäftsbücher einen Zeitrahmen von zehn Jahren. In Anbetracht dessen, rechtfertigt sich auch hier eine Festlegung der Frist auf 10 Jahre. Wir beantragen deshalb die Aufnahme einer entsprechenden Präzisierung ins Gesetz.

SWICO Zu Abs. 2: Genügt dieser allgemeine Wortlaut oder sollte dieser nicht näher spezifiziert werden? Mit einer Spezifikation würde die Rechtssicherheit hinsichtlich Art. 17 Abs. 1 etwas geklärt und zudem den Sorgfaltsmassstab erhöhen. Damit würde auch die Qualität des EDV-Systems in sicherheitsmässiger Hinsicht gesteigert werden können.
Zwecks Wahrung der Flexibilität könnte diese Präzision auch in die Ausführungsvorschriften aufgenommen werden, indem Abs. 2 um den nachfolgend eingefügten, kursiv gesetzten Text ergänzt würde; also: „*... ihnen den Anforderungen der Ausführungsvorschriften genügende Massnahmen zur Geheimhaltung ..“.*
Zu Abs. 3: Falls Beizug von Dritten vorgesehen (z.B. Registrierstellen), wäre diesem Umstand im Wortlaut dieses Absatzes Rechnung zu tragen - so etwa hinsichtlich der Aufbewahrung der Dokumentation durch den Dritten (oder deren Aushändigung an die Zertifizierungsstelle) und das Recht um Einsicht bzw. Auskunft der Zertifizierungsstelle.

321.11 Art. 11

Kantone / Cantons / Cantoni

BE Wir erachten die Frist von drei Tagen als ungenügend, um die notwendigen Abklärungen zu treffen. Wir schlagen vor, die Frist auf fünf Tage zu erstrecken.

GE Selon l'art. 11, al. 3, la durée de la suspension de la validité d'un certificat électronique serait au maximum de trois jours, qui, d'après le rapport explicatif, seraient tant des jours ouvrables que non ouvrables. Ce rapport n'explique pas suffisamment la justification de la brièveté d'une telle durée de suspension, et n'apporte pas d'éléments qui convainquent de l'applicabilité du système prévu à cet égard.
Il nous paraît par ailleurs manquer d'indications sur le *dies a quo* de la suspension considérée, ainsi que sur les conséquences d'une telle suspension.

SG Wir beantragen, in Art. 11 Abs. 1 einen neuen Bst. a^{bis} mit folgendem Wortlaut einzufügen: „ *deren Inhaberin oder Inhaber gestorben ist.“*
Begründung: Aus Gründen der Rechtssicherheit ist das elektronische Zertifikat mit dem Tod seiner Inhaberin oder seines Inhabers ungültig zu erklären.
Wir beantragen, den Tatbestand von Art. 11 Abs. 1 Bst. c mit der Rechtsfolge des Entzugs der Anerkennung der Anbieterin von Zertifizierungsdiensten zu verknüpfen (Art. 4 Abs. 1 Bst. f i.V.m. Art. 15). Die entsprechende Bestimmung ist an geeigneter Stelle einzufügen.

Begründung: Kann eine Anbieterin von Zertifizierungsdiensten keine Gewähr für die Zuordnung eines öffentlichen Schlüssels zu einer bestimmten Person mehr bieten, erfüllt sie ihre wichtigste definitionsgemässe Aufgabe nicht mehr.

VD Il paraîtrait opportun de régler expressément les conditions d'annulation en cas de décès du titulaire du certificat. A l'al. 3, il faudrait préciser quelles mesures doivent être prises en cas de doute sur la validité d'un certificat, durant les trois jours de suspension.
Avant l'annulation d'un certificat, il se pose aussi la question du droit d'être entendu du titulaire.

ZG Gemäss Art. 11 Abs. 1 Bst. a kann die Inhaberin oder der Inhaber eines elektronischen Zertifikats einen Antrag auf Ungültigerklärung eines solchen Zertifikats stellen. Auch Abs. 3 und 4 sprechen von der sogenannten Ungültigerklärung. Abs. 2 sollte unseres Erachtens daher diese Terminologie übernehmen und folgendermassen angepasst werden: *„Bei der Ungültigerklärung auf Antrag (Abs. 1 Bst. a), müssen sie sich vergewissern, dass die Person, welche die Ungültigerklärung beantragt, dazu berechtigt ist."*

Parteien / Partis / Partiti

FDP Es muss sichergestellt sein, dass die Dauer der Aufbewahrungspflicht der Revocation-Liste sowie die Rechtswirkungen dieser Liste auf bereits abgeschlossene Rechtsgeschäfte in den Ausführungsvorschriften (Art. 23) bzw. durch Hinweise auf die entsprechenden Regelungen des OR für den Rechtssuchenden klar ersichtlich sind.

Organisationen / Organisations / Organizzazioni

Briner Wir vermögen nicht zu ersehen, weshalb die Möglichkeit einer Suspension auf 3 Tage beschränkt wird. Das ist einerseits (zum Beispiel über Ostern oder Weihnachten) zu kurz, und andererseits verhindert der Entwurf nicht die beliebige Erneuerung einer Suspension.
Wir glauben nicht, dass es damit getan ist zu sagen, im Falle der Aufhebung einer Suspension habe diese „keine Wirkung" (Abs. 3 in fine). Wenn die Suspension wirksam greifen soll, muss sie einen Einfluss auf Geschäfte haben, die in dieser Zeit abgeschlossen worden sind. Es ist ja keineswegs auszuschliessen, dass ein signiertes Dokument während dieser drei Tage beim Empfänger „liegenbleibt".

CP L'annulation des certificats devra se faire rapidement vu la vitesse à laquelle les transactions se font sur le web. Cela pourra se faire de manière volontaire ou non. Un délai de suspension (trois jours) est prévu en cas de doute. Cette procédure est nécessaire vu l'importance que revêt la signature électronique.

economiesuisse Die in Abs. 3 vorgeschlagene maximale Dauer für die Suspendierung von Zertifikaten von drei Kalendertagen ist zu kurz. Sie ist auf mindestens fünf bis zehn Tage zu verlängern.

FGSec Zu Abs. 3: Es sollte klar geäussert werden, dass der Nutzer innert (z.B.) 3 Tagen reagieren muss, da ansonsten sein Zertifikat revoziert wird.

FHZ Hier ist an dieser Stelle zu präzisieren, wie lange diese Revocationliste aufbewahrt werden muss und welche Rechtswirkung die Revocation, insbesondere eine nach lit. b und c, auf früher abgeschlossene Rechtsgeschäfte hat.

Muster/Sury Nicht geregelt ist, was zu unternehmen ist, wenn der Signierschlüssel der Zertifizierungsstelle kompromittiert worden ist. z.B. sind die Primfaktoren der RSA Moduli im Internet publiziert worden.

SBV La durée maximale de suspension du certificat, fixée à l'art. 11 al. 3, pourrait être portée à cinq voire dix jours. Pour des raisons tenant à la sécurité du droit et des transactions, une suspension illimitée du certificat - pour peu qu'une solution allant dans ce sens soit envisagée - nous paraîtrait toutefois inappropriée. Se pose en outre la question de savoir qui assume la responsabilité résultant d'un dommage qui se produit entre le moment où la demande de révocation parvient au fournisseur de services de certification et celui où la révocation est publiée.

SIK Hier (oder an einer anderen Stelle) fehlt ev. eine Bestimmung, die regelt, wie es sich beim Tod, Bevormundung etc. verhält, es sei denn, dass andere Gesetzeswerke diese Fälle eindeutig abdecken. Der Tote, z. B., unterschreibt sicher nicht mehr, sein Zertifikat ist aber noch gültig, brauchbar und nicht mehr unter der Aufsicht seines Inhabers nach Art. 16, im Gegensatz zur „Papier-Unterschrift".

SVV Abs. 3: „Bestehen bezüglich der Gültigkeit des Zertifikats Zweifel, so kann dieses für die Dauer von maximal *zehn* Tagen suspendiert werden. Nach Ablauf dieser Frist erklären die Anbieterinnen von Zertifizierungsdiensten die Zertifikate definitiv für ungültig oder erneut für gültig. Im ersten Fall wird die Ungültigerklärung im Zeitpunkt der Suspendierung des Zertifikats wirksam; im zweiten Fall hat die Suspendierung keine Wirkung auf die Gültigkeit des Zertifikats."

Begründung: Abs. 3 der Bestimmung verlangt, dass bei Zweifeln an der Gültigkeit eines Zertifikats, dieses für maximal drei Tage suspendiert werden kann. Es versteht sich, dass eine seriöse Abklärung der Richtigkeit eines Zertifikates je nach Umstand innerhalb dreier Tage kaum möglich sein wird. Gerade bei einer missbräuchlichen Verwendung wird der falsche Inhaber aus eigenem Interesse die Rechercheaktivitäten des Zeritifizierungsdienstanbieters zu verhindern versuchen. Die Frist von drei Tagen erscheint unter dieser Optik zu kurz zu sein. Da die Suspendierung faktisch die Wirkung hat, dass ein Zertifikat temporär als ungültig zu betrachten ist, ist auch nicht ersichtlich, warum dieser Status nur so kurzfristig aufrecht erhalten werden sollte. Der Anbieter einer Dienstleistung andererseits hat ein Interesse an der Beendigung des schwebenden Zustandes. Es rechtfertigt sich folglich eine angemessene Frist anzusetzen. Wir halten 10 Tage für angemessen und beantragen eine entsprechende Ausdehnung der Frist.

SWICO Der Titel ist falsch, es wird auch die Suspendierung geregelt. Diese ist bei geschlossenen Systeme wohl üblich, bei qualifizierten Zertifikaten unüblich und gefährlich. Eine saubere Regelung der Reaktivierung ist zudem nicht ganz unproblematisch und umständlich/aufwändig. Die Suspendierung ist deshalb zu streichen. Die Suspendierung wurde deshalb weder in der EU-Richtlinie noch im deutschen SigG vorgesehen.

Die Fristüberschneidung in Abs. 3 führt zu Konflikten (vgl. § 8 deutsches SigG „eine rückwirkende Sperrung ist unzulässig"). Hier müsste zudem eine spezielle Haftungsregelung stehen!

Abs. 1 lit. b: Wer haftet, wenn die Gültigkeit des Zertifikats nicht mehr gegeben ist und sich dies aber erst später herausstellt?

Abs. 2 ist sicherheitstechnisch völlig inakzeptabel. Die Berechtigungsprüfung muss immer in einer alternativen Weise, d.h. nicht mit der im Zweifelsfall korrupten Signatur, vorgenommen werden.

Vischer Der Gesetzesentwurf sieht vor, dass ein Signaturschlüssel (bzw. ein für einen bestimmten Schlüssel ausgestelltes Zertifikat) für ungültig erklärt werden kann (Art. 11). Eine Ungültigerklärung kommt in erster Linie in Frage, wenn der

Inhaber des Signaturschlüssels dies beantragt, etwa weil er vermutet, dass Unbefugte in den Besitz einer Kopie des Schlüssels gelangt sind.
Hinter der Möglichkeit, einmal ausgestellte Schlüsselzertifikate nachträglich für ungültig erklären zu lassen, verbirgt sich ein fundamentales Problem, das im Begleitbericht zur Vernehmlassungsvorlage mit keinem Wort angesprochen wird.
Zunächst gilt Folgendes: Die an eine Computer-Datei, etwa eine E-Mail-Nachricht, angefügte elektronische Signatur belegt zweifelsfrei, dass das betreffende Dokument seit der Anbringung der Signatur nicht mehr verändert wurde (Authentizitätsgarantie). Davon ausgehend, dass nur der registrierte Inhaber der Signatur im Besitz des betreffenden Schlüssels und damit zur Generierung der Signatur in der Lage ist, wird darauf geschlossen, dass nur diese Person das Dokument signiert haben kann. Der Inhaber der an das Dokument angefügten Signatur kann seine Autorschaft nicht abstreiten, er muss sich im Rechtsverkehr den Inhalt dieses Dokuments entgegenhalten lassen.
Nun ist aber zu beachten, dass nicht zuverlässig festgestellt werden kann, zu welchem Zeitpunkt eine elektronische Signatur an ein bestimmtes Dokument angebracht wurde (vgl. Begleitbericht, S. 26). Konkret bedeutet das, dass von einer digital signierten E-Mail-Nachricht nicht zuverlässig festgestellt werden kann, an welchem Datum und zu welcher Zeit diese signiert und verschickt wurde. Zwar enthalten E-Mail-Nachrichten in der Regel entsprechende, von den Übermittlungsservern automatisch eingefügte Zeitangaben im Kopfteil („Header“), aber diese Zeitangaben sind von der Authentizitätsgarantie der elektronischen Signatur nicht mit abgedeckt und können deshalb relativ einfach manipuliert werden.
Ein geschäftsreuiger Autor einer im Rechtsverkehr abgegebenen Verpflichtungserklärung hat demnach die Möglichkeit, nach dem Versand einer von ihm digital signierten E-Mail-Nachricht sein Schlüsselzertifikat für ungültig erklären zu lassen und anschliessend zu behaupten, die betreffende Nachricht sei erst nach dem Zeitpunkt der Ungültigerklärung des Schlüsselzertifikates digital signiert worden, weshalb ihm die Signatur nicht zugerechnet werden könne und er an die in der betreffenden Nachricht abgegebenen Erklärungen nicht gebunden sei. In technischer Hinsicht kann in einer solchen Situation nicht zuverlässig nachgewiesen werden, dass die Signierung in Wirklichkeit zu einem Zeitpunkt erfolgte, als das Schlüsselzertifikat noch gültig war.
Für die praktische Verwendung der elektronischen Signatur hat dies die folgende Konsequenz: Wer eine digital signierte Nachricht erhält und sicherstellen will, dass er im Falle eines späteren Streits den Erhalt der mit einer gültigen Signatur versehenen Nachricht beweisen kann, muss nicht nur die signierte Nachricht aufbewahren, sondern zusätzlich noch den Zeitpunkt des Erhalts dieser Nachricht prozesswirksam festhalten. Dies könnte etwa so geschehen, dass der Empfänger die betreffende Nachricht auf einen mobilen Datenträger (etwa eine Diskette oder eine CD-ROM) kopiert und diesen Datenträger bei einem Notar deponiert. Denkbar wäre auch, dass der Empfänger der Nachricht sich sofort von der Akkreditierungsstelle eine Bestätigung im Sinne von Art. 21 Abs. 1 ausstellen lässt. Beide diese Möglichkeiten sind für die Praxis des täglichen Geschäftsverkehrs unbrauchbar. Eine elektronische Signatur erfüllt ihren Zweck nur dann, wenn der Empfänger einer signierten Nachricht zur Sicherung der Beweislage nicht mehr tun muss, als diese aufzubewahren; jeder Mehraufwand ist unpraktikabel. Dies führt zu folgendem Schluss: Der Umstand, dass der Zeitpunkt des Versandes einer elektronischen Signatur im Nachhinein nicht

zuverlässig festgestellt werden kann, verbunden mit der Möglichkeit, dass ein bestimmter Signaturschlüssel jederzeit pro futuro für ungültig erklärt werden kann, lässt den Beweiswert einer elektronischen Signatur unter die Schwelle des im Geschäftsverkehr Akzeptablen sinken.
Im Begleitbericht zur Vernehmlassungsvorlage wird mit Recht darauf hingewiesen, dass die technische Möglichkeit besteht, den Beweiswert einer elektronischen Signatur insofern zu erweitern, als bei der Übermittlung einer digital signierten Nachricht ein von einer autorisierten Stelle zertifizierter „Zeitstempel" (time stamping) angebracht werden kann (Begleitbericht, S. 26). Mit einem solchen „Zeitstempel" könnten die oben geschilderten Vorbehalte beseitigt werden. Es wäre denkbar, im Gesetz festzulegen, dass die für elektronische Signaturen vorgesehenen Rechtswirkungen nur dann eintreten, wenn die signierte Erklärung mit einem solchen „Zeitstempel" versehen ist. Die Vernehmlassungsvorlage sieht dies jedoch (ohne nähere Begründung) nicht vor.

321.12 Art. 12

Kantone / Cantons / Cantoni

BS Nach dieser Bestimmung darf neben den Kosten für die Nutzung der öffentlichen Fernmeldedienste kein weiteres Entgelt verlangt werden. Neben öffentlichen Fernmeldediensten gibt es nun auch private. Daher stellt sich die Frage nach der Zulässigkeit der Weiterverrechnung der Kosten der Nutzung der privaten Fernmeldedienste.

SG Wir beantragen, Art. 12 Abs. 3 Satz 2 wie folgt zu formulieren: „*Sie verlangt dafür* kein weiteres Entgelt".
Begründung: Der Begriff der öffentlichen Fernmeldedienste wird dem raschen technischen und rechtlichen Wandel im Bereiche der Telekommunikation nicht gerecht und ist entbehrlich.

Parteien / Partis / Partiti

PLS Les listes de certificats électroniques revêtent une importance cruciale, surtout en cas d'annulation ou de suspension. Il faudrait donc prévoir dans le texte de loi que des moyens techniques appropriés doivent être mis en place pour assurer la protection de ces listes.

FDP Vgl. zu Art. 11 / Cf. ad art. 11 / Cfr. ad art. 11.

Organisationen / Organisations / Organizzazioni

camera commercio Wie / Comme / Come DigiSigna.

CP Les fournisseurs de services électroniques doivent tenir à jour une liste des certificats émis, annulés ou suspendus. Cette obligation répond au souci de garantie lié aux certificats. Ils doivent également assurer la protection des données personnelles de leurs clients. Cela paraît tout à fait logique.

DigiSigna Zu Abs. 3: Die Forderung nach einem unentgeltlichen Zugang ist systemwidrig. Es muss dem Zertifizierdiensteanbieter überlassen bleiben, ob er den Aufwand für die Registerführung über den Preis des Zertifikates abdecken will, oder ob er eine Gebühr für die Abfrage erheben will. Zudem würde diese Forderung den Grossbezüger von Validierungsabfragen zulasten des gelegentlichen Benutzers begünstigen. In der Praxis wird wohl die gelegentliche Einzelabfrage unentgeltlich sein, jedoch die regelmässige Zustellung von Revokationsinformationen gebührenpflichtig sein. Die ersatzlose Streichung des zweiten Satzes in Abs. 3 ist deshalb absolut notwendig, damit ein Zertifizierdienst überhaupt wirtschaftlich angeboten werden kann.

economiesuisse In der Botschaft ist darauf hinzuweisen, dass die gemäss Abs. 1 und Abs. 2 vorgeschriebenen Verzeichnisse – falls elektronisch geführt – unbedingt geschützt werden müssen. Die Personen, die sich auf diese Verzeichnisse abstützen, sollen sich auf deren Authentizität verlassen dürfen. Die entsprechenden Anforderungen sind sodann in den Ausführungsvorschriften zu regeln.

Von den Anbietern wird das Erfordernis der Gewährung eines unentgeltlichen Zuganges zu den Registern der Zertifizierungsstellen kritisiert. Erstens erscheint diese Kostenregelung ungünstig, weil sie die Zertifikate für den privaten Nutzer erheblich verteuert und damit die erfolgreiche Durchsetzung des neuen Systems behindern könnte. Zweitens gibt es für eine solche Regelung auch keine Notwendigkeit. Allfälligen Missbräuchen kann mit wettbewerbsrechtlichen Massnahmen begegnet werden. Ein Zugang zu geringen Kosten zu den Registern ist aus Gründen des Vertrauens andererseits gerade in der Einführungsphase zentral. Entsprechend wäre es wohl richtiger, diese Frage auf der Stufe der Verordnung zu regeln und im Gesetz nur einen Kompetenzartikel vorzusehen. Die Verpflichtung zur Kostenlosigkeit von Abfragen muss sich aber auf Einzelabfragen beschränken. Massenabfragen und systematisierte Abfrageroutinen müssen von den Anbietern mit Kosten belegt werden können. In Art. 12 muss zudem das Wort „öffentliche“ im Zusammenhang mit Fernmeldediensten gestrichen werden, da es bei der heutigen Liberalisierung nur zu Missverständnissen führt.

FGSec Terminologie: Der Begriff „Verzeichnis“ kann als technischer Termin namentlich für X.500- oder LDAP-Verzeichnisse verstanden werden, oder einfach als indizierte Liste von Daten. In Abs. 1 geht es um ein Verzeichnis im technischen Sinne; dasjenige von Abs. 2 muss kein Verzeichnis im technischen Sinne sein. Ausserdem muss es kein Verzeichnis der Zertifikate sondern nur ein Verzeichnis der Seriennummern sein. In Abs. 3 bezieht sich „den Verzeichnissen“ auf zwei unterschiedliche Objekte; der Begleitbericht ist in diesem Punkt auch verwirrend.

FHZ Vgl. zu Art. 11 / Cf. ad art. 11 / Cfr. ad art. 11.

kf *„...öffentliche..“* Fernmeldedienste streichen, diese Formulierung ist verwirrlich beim liberalisierten Markt.

SBV Les listes de certificats électroniques - en particulier de ceux ayant été annulés ou suspendus - revêtent une importance décisive. Il conviendrait dès lors de préciser, dans la loi ou dans l'ordonnance, que ces listes doivent être protégées par des moyens techniques appropriés.

La deuxième phrase de l'art. 12 al. 3, qui traite des frais liés à la consultation des listes, doit être supprimée. C'est aux fournisseurs de services de certification qu'il appartient de régler cette question, d'entente avec leurs clients. La concurrence entre les fournisseurs est par ailleurs de nature à apporter, dans ce domaine, une solution appropriée.

SWICO Im selben Sinne wie / Dans le même sens que / Nello stesso senso che economiesuisse.

swisscom Art. 12 Abs. 3, 1. Satz, des Entwurfs verpflichtet Anbieterinnen von Zertifizierungsdiensten *(*Certification Authority, CA), den elektronischen Zugang zu den Verzeichnissen zu gewährleisten. Das ist sinnvoll. Fraglich ist jedoch der 2. Satz des erwähnten Absatzes, wonach für diesen elektronischen Zugang neben den Kosten für die Nutzung der „öffentlichen Fernmeldedienste“ kein weiteres Entgelt verlangt werden dürfe. Die Bezeichnung „öffentliche Fernmeldedienste“ ist unklar. Seit dem per 1.1.98 in Kraft getretenen neuen Fernmelde-

gesetz gibt es - mit Ausnahme der Grundversorgung - keinen Tatbestand mehr, der so bezeichnet werden könnte. Sodann ist nicht ersichtlich, inwiefern ein solcher Eingriff in die Preisfestsetzungsfreiheit von CA gerechtfertigt ist. Es ist Aufgabe und Recht der CA, im Rahmen ihrer Produktepalette (u.a. Herausgabe von Zertifikaten und Verzeichnisdienste) entsprechende Preise festzulegen. Aus unternehmerischer Sicht kann es durchaus sinnvoll sein, den Preis für das Produkt A zu reduzieren und den Preis für das Produkt B zu erhöhen. Falls an einer diesbezüglichen Regulierung festgehalten wird, sollte klargestellt werden, dass die Unentgeltlichkeit nur für Einzelabfragen und nicht für das „Absaugen" ganzer Datenstämme gilt.

Swisskey Im Zusammenhang mit dem „unentgeltlichen" Zugang zu den Registern muss man klarstellen, dass Einzelabfragen kostenlos erfolgen können, jedoch Massenabfragen und weitergehende Dienstleistungen (Push-Service etc.) verrechnet werden können. Es ist in diesem Zusammenhang auch darauf hinzuweisen, dass die Abfrage beim Handelsregister hinsichtlich der Gültigkeit einer Prokura oder ähnlichem auch kostenpflichtig ist. Auch die Beglaubigung einer handschriftlichen Unterschrift durch einen vertrauenswürdigen Dritten (klassischerweise ein Notar) ist mit Kosten verbunden.

321.13 Art. 13

Kantone / Cantons / Cantoni

BS Wenn eine anerkannte Anbieterin von Zertifizierungsdiensten ihre Geschäftstätigkeit freiwillig einstellt, ist sie verpflichtet, die von ihr ausgestellten, noch gültigen elektronischen Zertifikate für ungültig zu erklären; die Akkreditierungsstelle beauftragt dann gemäss Art. 13 Abs. 2 Satz 2 eine andere anerkannte Anbieterin von Zertifizierungsdiensten, das Verzeichnis der für ungültig erklärten Zertifikate zu führen und weitere Handlungen vorzunehmen. Es stellt sich unseres Erachtens die Frage, ob die andere anerkannte Anbieterin von Zertifizierungsstellen verpflichtet ist, diesen Auftrag anzunehmen. Falls diese Pflicht nicht ohne weiteres besteht, müsste daran gedacht werden, die Bestimmungen in Art. 4 Abs. 1 so zu ergänzen, dass Personen anerkannt werden können, wenn sie : *„g. sich verpflichten, gegebenenfalls einen Auftrag gemäss Art. 13 Abs. 2 oder 3 anzunehmen".*

GE L'art. 13, al. 3 ne précise pas - sans toutefois l'exclure - si, en cas de faillite d'un fournisseur de services de certification reconnu, le fournisseur qui serait alors chargé par l'organisme d'accréditation d'accomplir un certain nombre de démarches (dont celle d'annuler les certificats électroniques non échus) pourrait ou non reprendre lui-même le „portefeuille" des certificats du fournisseur en faillite. Cela nous paraît soulever la question de savoir si un tel „portefeuille" aurait une valeur marchande ou non dans le cadre de la liquidation de la faillite.

SG Wir beantragen, in den Ausführungsvorschriften über die Aufbewahrung der Angaben zu elektronischen Zertifikaten eine grosszügige Frist vorzusehen.
Begründung: Es darf nicht sein, das Dokumente oder Vertragsabschlüsse nach einiger Zeit - aus technischen oder organisatorischen Gründen – ihre Signatur „verlieren" bzw. das zugrundeliegende elektronische Zertifikat nicht mehr nachvollziehbar ist.

TI Nell'ottica della trasparenza, ci sembra importante che il titolare della chiave privata sia subito informato in caso di cessazione dell'attività del prestatore di servizi di certificazione (art. 13), rispettivamente in caso di trasferimento della proprietà azionaria.

VD L'al. 3 devrait prévoir que l'administration de la faillite informe l'organisme d'accréditation dès que possible. Une telle obligation devrait être indiquée dans la législation d'application de la loi sur la poursuite pour dettes et la faillite.

ZG Art. 13 regelt die Folgen der Einstellung der Geschäftstätigkeit. Nicht geregelt ist der Tatbestand der Fusion von anerkannten Anbieterinnen. Muss in einem solchen Fall eine Privatperson eine neue digitale Signatur bestellen und dafür eventuell nochmals einen ansehnlichen Beitrag leisten und die bereits anerkannte Anbieterin für eine Neuanerkennung nochmals eine Gebühr entrichten?

Organisationen / Organisations / Organizzazioni

CP La procédure proposée en cas de cessation d'activité d'un fournisseur de services de certification nous paraît judicieuse.

economiesuisse Wer trägt die Folgen, wenn bei Geschäftsaufgabe die Zertifikate nicht für ungültig erklärt werden? Wer trägt die Kosten für die Ungültigkeitserklärung der Zertifikate und für die Führung der Liste? Es kann doch nicht sein, dass irgend eine Zertifizierungsstelle mit dieser „Aufräumarbeit" betraut wird und dann die Kosten erst noch selber tragen muss. Es sind daher die Abs. 2 und 3 mit folgendem Satz zu ergänzen:
Abs. 2: „... sowie die entsprechenden Belege aufzubewahren. Die Versicherung gemäss Art. 4 Abs. 1 lit. e deckt die dadurch verursachten Kosten."
Abs. 3: „... sowie die entsprechenden Belege aufzubewahren. Die Versicherung gemäss Art. 4 Abs. 1 lit. e deckt die dadurch verursachten Kosten."
Zudem stellt sich für uns die Frage, wie im Falle von Abs. 3 vorzugehen ist, wenn es keine Zertifizierungsstelle mehr in der Schweiz gibt, was sogar sehr wahrscheinlich sein dürfte, ist doch der schweizerische Markt sehr klein.

FGSec Zu Abs. 2: Sind akkreditierte CSPs verpflichtet, die CRLs und Logs eines anderen CSPs zu führen, der seine Geschäftstätigkeit eingestellt hat? Wer entscheidet, zu welchem Preis dies zu geschehen hat?

Abs. 3 stellt ein Problem dar, da ein X.509-Zertifikat den CRL-Issuer spezifiziert (optionales Attribut „CRL Distribution Point," oder „default Certificate Issuer"). Es ist nicht offensichtlich, wie *die relying party* überzeugt werden kann, dass der neue CRL Ausgeber „authoritative" ist - im Besonderen wenn der Nachschlag in der CRL automatisiert wurde. Eine Umleitung zum neuen Aussteller ist einfach, aber ändert die Ausstellerinformation nicht.

ISACA Erklärt der Art. 11 einerseits die Notwendigkeit und Voraussetzungen zur Ungültigkeitserklärung von elektronischen Zertifikaten auf der Basis eines Antrages durch Inhaberinnen oder Inhaber missbräuchliche Erlangung oder Verlustes der Vertrauenswürdigkeit eines elektronischen Zertifikates, wird mit dem Art. 13 wohl eine Ungültigkeitserklärung der elektronischen Zertifikate gefordert ohne aber einen ersichtlichen Grund dafür anzugeben. Ferner wird nicht - wie im Art. 11 gefordert - eine Information der Inhaberinnen und Inhaber von betroffenen elektronischen Zertifikaten erwogen. Mit der Ungültigkeitserklärung nimmt man offensichtlich auch in Kauf, dass eine Person für einen bestimmten Zeitraum über keine beglaubigte digitale Signatur verfügt.
Revoir cette procédure dans le sens suivant: Gemäss den Ausführungen zu Art. 4 haben Anbieterinnen von Zertifizierungsdiensten gewisse Auflagen zu erfüllen. Diese Anforderungen sollten nicht nur zum Erhalt einer Anerkennung notwendig sein, sondern deren Einhaltung sollte auch im Nachhinein jederzeit durch entsprechende Revisionsstellen (et les organismes de reconnaissance) überprüft werden. Eine Anbieterin sollte bis zur Einstellung der Geschäfts-

tätigkeit die Einhaltung der unter Art. 11 aufgeführten Möglichkeiten zur Ungültigkeitserklärung der elektronischen Zertifikate gewährleisten.
Faire un renvoi à l'obligation d'informer les titulaires des certificats prévue à l'art. 11, al. 4.

SBV Lorsqu'un fournisseur de services de certification cesse d'exercer son activité, le projet prévoit que l'organisme d'accréditation charge un autre fournisseur de tenir la liste des certificats annulés ou de conserver les certificats annulés ou échus. Le projet ne donne toutefois aucune indication sur la répartition des coûts en résultant. Nous proposons dès lors de compléter les al. 2 et 3 de l'art. 13 par l'indication suivante:
(…) „Les assurances contractées conformément à l'article 4 alinéa 1 lit. e couvrent les coûts en résultant".
(…) „Die Versicherung gemäss Art. 4 Abs. 1 lit. e deckt die dadurch verursachten Kosten".

KVN Bei einer freiwilligen Geschäftsaufgabe von Zertifizierungsdiensten sollten diese Anbieterinnen gesetzlich verpflichtet werden, dafür zu sorgen, dass die Übernahme der elektronischen Zertifikate für die noch bezahlte Gültigkeitsdauer ohne Kostenfolge für die Konsumenten durch eine andere anerkannte Anbieterin von Zertifizierungsdiensten gewährleistet ist.
Begründung: Andernfalls können solche Anbieterstellen kurzfristig nach der Eröffnung bei lukrativen Auftragseingängen ihre Geschäfte wieder schliessen und ihre Kunden um die ihnen zustehende Dienstleistung ohne finanziellen Schaden prellen.

Muster/Sury Bei Konkurs kann die Ungültigkeitserklärung der Zertifikate einen beträchtlichen Schaden für die Unternehmen verursachen, deren Mitarbeiter alle Zertifikate bei ein und derselben Zertifizierungsstelle haben, welche ihre Geschäftstätigkeit einstellt. Zwischen der Einstellung der Geschäftstätigkeit und der Ungültigkeitserklärung sollte eine angemessene Frist von 3-4 Monaten angesetzt werden. (Unter anderem auf Grund der Notwendigkeit dieser Anforderung sollte die Anerkennung einer Zertifizierungsstelle einer strengen polizeilichen Bewilligung gleichkommen und nicht privatrechtlich geregelt werden. Ebenfalls die Aufsicht der Zertifizierungsstelle sollte klar geregelt werden!)
Es stellt sich die Frage, ob eine Zertifizierungsstelle die Pflicht hat, den Auftrag nach Abs. 3 anzunehmen und auszuführen, also einem Kontrahierungszwang unterliegt. Es kann je nach SW für das Zertifikatsausstellen ein Ding der Unmöglichkeit sein, dies technisch zu realisieren. Verschiedene Zertifizierungsstellen haben nämlich je unterschiedliche Signierschlüssel. Wollte eine Zertifizierungsstelle dieser Anforderung gerecht werden, dann müsste sie den Import von fremden CA Schlüsseln ermöglichen und den Signierschlüssel wahlweise bestimmen können. Ist dies technisch nicht realisierbar, dann müsste die neue Zertifizierungsstelle Personal bereitstellen, um die in Konkurs fallende Zertifizierungsstelle weiterhin zu betreuen.

SVV Abs. 2 sieht im Falle der Einstellung der Geschäftstätigkeit einer Zertifizierungsdiensteanbieterin vor, dass die Akkreditierungsstelle eine andere anerkannte Anbieterin beauftragt, das Verzeichnis der für ungültig erklärten Zertifikate zu führen und die abgelaufenen oder für ungültig erklärten Zertifikate, das Tätigkeitsjournal sowie die entsprechenden Belege aufzubewahren. Ohne dass dieser Umstand für die Privatassekuranz je ein Thema sein dürfte, versteht sich, dass die bei einer Zwangsübernahme entstehenden Unkosten gedeckt

sein sollten. Wir beantragen deshalb einen Zusatz im Gesetzestext, der diesem Anliegen Rechnung trägt.

SWICO Abs. 2: Der Lösungsansatz ist falsch. Die Tatsache, dass eine Zertifizierungsstelle ihre Geschäftstätigkeit aufgibt, bedeutet nicht, dass die Zertifikate deswegen weniger vertrauenswürdig sind. Insofern ist die Ungültigkeitserklärung gemäss Abs. 2 nicht notwendig und führt zu unnötigem Aufwand und u.U. zu grossen logistischen Problemen (man stelle sich vor, es müssten kurzfristig 2 Mio. Chipkarten ausgetauscht werden, das ist weder technisch noch organisatorisch machbar). Sollte der Fall eintreten, dass keine Zertifizierungsinstanz mehr vorhanden ist, muss die Akkreditierungsstelle dafür einstehen.

Sodann ist hinsichtlich der Frage, wer die Kosten bei solchen Vorfällen zu tragen hat, zu regeln. Denn, es kann doch nicht sein, dass irgend ein Anbieter von Zertifizierungsdiensten mit dieser „Aufräum"arbeit betraut wird und dann die Kosten erst noch selber tragen muss!

Abs. 2 sollte somit ergänzt werden wie folgt: „... die entsprechenden Belege aufzubewahren. *Die Versicherung gemäss Art. 4 Abs. 1 lit. e deckt die dadurch verursachten Kosten*."

Abs. 3 sollte somit ergänzt werden wie folgt: „... sowie die entsprechenden Belege aufzubewahren. *Die Versicherung gemäss Art. 4 Abs. 1 lit. e deckt die dadurch verursachten Kosten*."

Swisskey Unklar ist dieser Artikel in seiner Bedeutung. Aufgrund der allgemeinen gesetzlichen Aufbewahrungspflichten müssen verschiedene Dokumente - so auch elektronische mit digitalen Signaturen versehene - über einen längeren Zeitraum aufbewahrt werden. Es muss daher sichergestellt werden, dass auch die Zertifikate (auch abgelaufene) für diesen Zeitraum zur Verfügung stehen. Wie möchte man dies bei der Aufgabe der Geschäftstätigkeit einer Anbieterin in bezug auf ihre Zertifikate sicherstellen? Konkret würde dies bedeuten, dass die „überlebende" Zertifizierdiensteanbieterin die Systeme der anderen weiterbetreiben müsste, um dies sicherstellen zu können. Probleme - wie zum Beispiel die Beschaffung einer Lizenz zwecks Betrieb des Systems des (geschäftsaufgebenden) Zertifizierungsanbieters - sind ungelöst.

321.14 Art. 14

Kantone / Cantons / Cantoni

SG Wir beantragen, Art. 14 Abs. 1 wie folgt zu formulieren: *„Die anerkannten Anbieterinnen von Zertifizierungsdiensten dürfen diejenigen Personendaten bearbeiten, die zur Erfüllung ihrer Aufgaben notwendig sind."*

Begründung: Angleichung der Formulierung an Art. 3 Bst. e des Bundesgesetzes über den Datenschutz, wonach als Bearbeiten jeder Umgang mit Personendaten gilt, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.

Organisationen / Organisations / Organizzazioni

Briner Wir sind nicht glücklich mit der Verweistechnik. In Art. 14 Abs.1 wird der Eindruck erweckt, es werde schlicht aus dem DSG zitiert bzw. eine datenschutzrechtliche Selbstverständlichkeit festgehalten, während der Begleitbericht (sachlich übrigens nicht notwendigerweise richtig) sagt, damit würden die Befugnisse der ZertD-Anbieterinnen beschränkt. Das müsste klar(er) gesagt werden.

CP Vgl. zu Art. 12 / Cf. ad art. 12 / Cfr. ad art. 12

economiesuisse Abs. 1 ist wie folgt zu ergänzen: *„Die anerkannten Anbieterinnen von Zertifizierungsdiensten und die von ihnen beauftragten Registrierungsstellen (Art. 9 Abs. 2) dürfen diejenigen Personendaten...“*
Da diese Bestimmung, laut Begleitbericht, das Datenschutzgesetz in einschränkender Weise präzisiert, sollten auch die Registrierstellen darin Erwähnung finden. Andernfalls liefen sie Gefahr, mit ihrer Tätigkeit das DSG zu verletzen.

FGSec Es muss eine Basis festgelegt werden, um zu einer einheitlichen Bestimmung der eindeutigen Namensgebung zu gelangen, z.B. Name, Vorname, Stadt, Land, Geburtsdatum, E-Mail-Adresse oder Name, Vorname, Land, AHV-Nr. etc.

FRC *„Il est interdit aux fournisseurs de services de certification reconnus de faire du commerce avec les données personnelles recueillies".*
En tant qu'organisation de défense des consommateurs, cette précaution nous paraît indispensable quand on sait qu'Internet ne connaît pas de frontières et que les données peuvent être assez sensibles (conclusion d'une assurance-vie via Internet).

kf Ergänzung: „Der Handel mit Personendaten ist für AnbieterInnen von Zertifizierungsdiensten untersagt.“
Das Datenschutzgesetz erlaubt grundsätzlich die Weitergabe von Personendaten (z.B. E-Mail-Adresse). Aus unserer Sicht sollte jedoch der Handel mit Daten für Zertifizierungsdienstanbieter grundsätzlich untersagt werden.

KVN Hier muss ausdrücklich festgehalten werden, dass den Anbieterinnen von Zertifizierungsdiensten jeglicher Handel mit Adressenmaterial strikte untersagt ist.

SBV L'obligation d'observer la législation sur la protection des données devrait s'étendre non seulement aux fournisseurs de services de certification, mais également aux bureaux d'enregistrement. Nous vous renvoyons à ce sujet à notre commentaire relatif à l'art. 9. A cet effet, l'art. 14 al. 1 pourrait être complété comme suit:
„Les fournisseurs de services de certification reconnus et les bureaux d'enregistrement mandatés par ceux-ci ne peuvent recueillir et traiter que les données personnelles…“.
„Die anerkannten Anbieterinnen von Zertifizierungsdiensten und die von ihnen beauftragten Registrierungsstellen dürfen diejenigen Personendaten…“

SWICO Laut Erläuterungen schränkt diese Bestimmung den Datenschutz gemäss DSG Art. 4 Abs. 3 ein. Diese Datenschutzbestimmung müsste wohl auch auf einen zulässigerweise beigezogenen Dritten (z.B. Registrierstelle) ausgedehnt werden.
Entsprechend schlagen wir folgende textliche Ergänzung vor: „Die anerkannten Anbieterinnen von Zertifizierungsdiensten und die von ihnen beauftragten Registrierungsstellen dürfen diejenigen Personendaten ….“
Die ganze Regelung ist zudem zu mager, wie am Beispiel des Verzeichnisdienstes bereits gezeigt wurde (Art. 12). Hier dürfte sich der Eidgenössische Datenschutzbeauftragte zu Wort melden.

321.15 Art. 15

Gerichte / Tribunaux / Tribunali

BGr Das Bundesgesetz über die elektronische Signatur sieht in Art. 15 eine Aufsicht der Anerkennungsstellen über die anerkannten Anbieterinnen von Zer-

tifizierungszertifikaten vor (vgl. auch Art. 5). Der Entzug der Anerkennung einer Anbieterin von Zertifizierungsdiensten wird gemäss Art. 15 Abs. 2 unverzüglich der Akkreditierungsstelle gemeldet. Der Gesetzesentwurf enthält indessen keine diesbezüglichen Rechtsschutzbestimmungen. Die Lücke wird auch durch das Bundesgesetz über die technischen Handelshemmnisse (SR 946.51), auf welches in einer Fussnote von Art. 15 Abs. 1 verwiesen wird, nicht geschlossen, da dieses Gesetz ebenfalls keine besonderen Rechtsschutzbestimmungen aufweist. Ohne solche Rechtsschutzbestimmungen gilt die ordentliche Rechtsmittelordnung nach dem Bundesgesetz über das Verwaltungsverfahren und dem Bundesrechtspflegegesetz. Damit der Gesetzesentwurf über die elektronische Signatur den laufenden Entlastungsbemühungen für das Bundesgericht entspricht, wonach das Bundesgericht grundsätzlich nicht mehr erste richterliche Instanz sein soll, ist gegen Verfügungen der Anerkennungsstelle der Beschwerdezug an eine eidgenössische Rekurskommission vorzusehen, die als Vorinstanz des Bundesgerichts entscheidet. Für rein technische Entscheidungen könnte unter Umständen vorgesehen werden, dass die eidgenössische Rekurskommission - bzw. später das unterinstanzliche Bundesverwaltungsgericht - letztinstanzlich entscheidet. Die Rechtsmittelordnung bedarf unter diesem Aspekt auf jeden Fall noch einer eingehenden Prüfung.

Organisationen / Organisations / Organizzazioni

CP Vgl. zu Art. 5 / Cf.ad art. 5 / Cfr. ad art. 5.

FSP Notre Fédération estime qu'il est capital de prévoir des dispositions efficaces en matière de surveillance et de transparence.
Nous déplorons la brièveté du projet sur ces points (une seule disposition au contenu laconique et peu explicite (cf. art. 15). Nous souhaitons que le projet soit complété et que les ordonnances d'application règlent judicieusement ces questions.

ISACA La surveillance exercée par les organismes de reconnaissance selon les normes d'accréditation (CB) est essentielle au bon fonctionnement du système.
Contrairement aux fournisseurs de service de certification reconnus (CA), les organismes de reconnaissance selon les normes d'accréditation (CB) ne répondent pas explicitement du dommage qu'ils causent lorsqu'ils violent les obligations que leur impose la loi.
La responsabilité des organismes de reconnaissance selon les normes d'accréditation (CB) pour le dommage qu'ils causent lorsqu'ils violent les obligations que leur impose la loi doit être explicitement prévue dans la loi, de manière comparable à l'art. 18 al. 1 pour les fournisseurs de service de certification reconnus (CA).

SUISA Vgl. zu Art. 5 / Cf. ad art. 5 / Cfr. ad art. 5.

321.16 Art. 16

Kantone / Cantons / Cantoni

AR Vgl. zu Art. 10 / Cf. ad art. 10 / Cfr. ad art. 10.

BE In Anbetracht der in Art. 17 Abs. 1 (zu Gunsten des Dritten, welcher auf ein Zertifikat vertraut hat) erlassenen Beweislastumkehr zu Lasten des Inhabers eines privaten Signaturschlüssels scheint es uns dringend angezeigt, den Begriff der Zumutbarkeit in Art. 16 Abs. 2 etwas enger zu fassen bzw. gesetzlich oder zumindest auf Verordnungsstufe zu konkretisieren. Insbesondere gilt es darauf hinzuweisen, dass die in Art. 10 Abs. 2 normierte Pflicht der anerkannten

Anbieter von Zertifizierungsdiensten, ihren Kunden geeignete Massnahmen zur Geheimhaltung des privaten Signaturschlüssels vorzuschlagen, in der Praxis zur Auslegung des Zumutbarkeitsbegriffs nach Art. 16 Abs. 2 herangezogen würde. Dabei darf es nicht angehen, dass die Anbieter durch die Strenge ihrer vorgeschlagenen Sicherheitsvorkehrungen die Grenze des zumutbaren Aufwandes selbst festlegen können. Dies würde dazu führen, dass vom Inhaber eines privaten Signaturschlüssels unter Umständen unverhältnismässige Anforderungen an sein Sicherheitskonzept gestellt und damit indirekt eine Kausalhaftung des Konsumenten begründet würde.
Schliesslich dürfte es auch im Interesse der Anbieter von Zertifizierungsdienstleistungen liegen, dass der Begriff der „zumutbaren Vorkehrungen“ konkretisiert wird. Unter Umständen könnten nämlich Schadenersatzklageverfahren wegen unzweckmässiger Instruktion/Information (bzw. wegen fehlender Wirksamkeit der vorgeschlagenen Sicherheitsmassnahmen) gestützt auf Art. 18 Abs. 1 i.V.m. Art. 10 Abs. 2 gegen die Anbieter geführt werden.
In diesem Sinne könnte sich die Beweislastverteilung des BGES ohne messbare gesetzliche Kriterien im Falle eines Missbrauchs sowohl für den Konsumenten als auch für die Anbieter von Zertifizierungsdiensten als Bumerang erweisen.

BL Unseres Erachtens sollte geprüft werden, ob Art. 16 mit einem Absatz zu ergänzen ist, wonach die Weitergabe des privaten Signaturschlüssels verboten ist. Damit würde die missbräuchliche Weitergabe zur Verwendung etwa im Rahmen der Geldwäscherei unter Strafe gestellt.

GE La question de la responsabilité des différents intervenants dans une infrastructure à clé publique est évidemment centrale. Les art. 16 à 19 du projet y sont consacrés et donnent, prima facie, une impression de cohérence d'ensemble. Plusieurs problèmes se posent néanmoins.
Ainsi, le titulaire de la clé privée peut se libérer de sa responsabilité s'il a adopté les „mesures qu'exigent les circonstances“ pour prévenir toute utilisation abusive d'un tiers. Il y a là évidemment source d'importants conflits, d'autant qu'à teneur de l'art. 10, al. 2 du projet, les fournisseurs de services de certification reconnus „doivent informer leurs clients des conséquences de la divulgation ou de la perte de leur clé privée, au plus tard lors de la délivrance des certificats électroniques. lis doivent leur indiquer les mesures appropriées pour maintenir leur clé privée secrète“. Qu'en sera-t-il si les mesures préconisées par le fournisseur de services de certification ont bien été suivies mais se révèlent objectivement insuffisantes?

GL Vgl. zu Art. 10 / Cf. ad art. 10 / Cfr. ad art. 10.

VS Le système de responsabilité préconisé (art. 16 ss) répartit correctement les risques liés aux transactions faites au moyen de signatures électroniques. Le devoir de diligence du propriétaire de la clé privée est clairement posé. Le renvoi au droit de la représentation (art. 32 ss CO) accompagné d'un renversement du fardeau de la preuve traitent avec sobriété et efficacité la délicate question des conséquences d'une utilisation abusive de la clé privée. Enfin, la responsabilité sans faute du fournisseur de services de certification avec obligation à sa charge de prouver qu'il a respecté les obligations résultant de la loi (renversement du fardeau de la preuve) apparaît comme une nécessaire conséquence de la spécificité de la technique d'authentification électronique.

ZH Die Haftung der Inhaberinnen und Inhaber privater Signaturschlüssel entfällt nach Art. 17 Abs. 3, wenn sie den Nachweis erbringen können, dass sie die in Art. 16 Abs. 2 geforderten Vorkehrungen getroffen haben. Im Begleitbericht wird

in diesem Zusammenhang zudem darauf hingewiesen, dass der Verlust des Schlüssels der Inhaberin oder dem Inhaber dann angelastet werden kann, wenn diese den Vorfall nicht umgehend den anerkannten Zertifizierungsdienstanbieterinnen gemeldet haben (S. 21). Das Unterlassen einer solchen Meldung kann damit analog der Verletzung der in Art. 16 Abs. 2 festgehaltenen Pflichten haftungsbegründend sein. Aus haftungsrechtlicher Sicht kann daraus eine eigentliche Meldepflicht abgeleitet werden. Rechts- und Verkehrssicherheit gebieten in diesem Fall, dass diese Meldepflicht in Art. 16 Abs. 2 auch ausdrücklich festgehalten wird. Konsequenterweise sollte zudem die in Art. 10 Abs. 2 geregelte Instruktionspflicht der anerkannten Anbieterinnen von Zertifizierungsdiensten um den Hinweis auf diese Meldepflicht erweitert werden.

Parteien / Partis / Partiti

PLS Il est primordial que le titulaire de la clé privée prenne toutes les mesures possibles pour maintenir le caractère secret de cette clé. Par conséquent, ce devoir de diligence devrait être décrit précisément dans l'ordonnance.

Organisationen / Organisations / Organizzazioni

Briner Es ist uns bewusst, dass die Haftung eine schwierige Frage ist. Trotzdem hinterlässt die Regelung im Entwurf insofern ein ungutes Gefühl, als einerseits in Art. 16 Abs. 2 statuiert wird, die unbefugte Verwendung müsse „ausgeschlossen" sein, während dann Art. 17 Abs. 3 davon ausgeht, dass eine unbefugte Verwendung ohne Haftung möglich ist. Dazuhin sagt der Begleitbericht (zu Art. 16), dass eine Haftung zum Beispiel dann entfalle, wenn ein Verlust umgehend gemeldet werde, was jedenfalls so nicht im Entwurf steht.

Unberücksichtigt bleibt sodann der Umstand, dass der Inhaber eines Signaturschlüssels einem Dritten dessen Verwendung erlauben kann und damit zivilrechtlich nicht nachlässiger handelt als jemand, der einem Dritten eine Vollmacht ausstellt, die im Innenverhältnis limitiert ist.

Es geht also nicht nur darum, die „Aufbewahrung" zu regeln. Es besteht ein subtiler Unterschied zwischen der „Verwendung durch unbefugte Drittpersonen" (gegenwärtig im Entwurf) und der „unbefugten Verwendung durch Drittpersonen". Ersteres ist etwas sehr signatur-spezifisches, weil man seinen Schlüssel im Gegensatz zu seiner Unterschrift unachtsam herumliegen lassen kann. Letzteres ist aber das, was in den Zusammenhang von Art. 38/39 OR gehört, der ja dann in Art. 17 Abs. 3 wieder aufgegriffen wird.

Insgesamt steht das Marginale von Art. 16 im Widerspruch zu einem Teil des Inhalts von Art. 16. Zudem sind wir aus demselben Grunde der Meinung, dass die Auflage an die ZertD-Anbieterinnen (die „nur" die Aufbewahrung anbelangt) gesetzestechnisch von derjenigen an die Inhaber zu trennen ist.

Clusis La question de la responsabilité des différents intervenants dans une infrastructure à clé publique est centrale. Les art. 16 à 19 du Projet y sont consacrés. A vrai dire, la manière dont cette question est réglée dans le Projet est discutable, en particulier aux motifs suivants.

De façon générale, une responsabilité n'est en jeu qu'en cas de préjudice résultant de la confiance indûment placée dans une signature électronique reposant sur un certificat dont la vérification n'a pas fait apparaître le caractère frauduleux. Sur cette base, le contenu du message transmis est faussement attribué au titulaire de la clé privée indiqué sur le certificat, alors que cette personne n'existe pas ou n'est pas celle qui a signé le message en question.

Dans une telle situation, on peut envisager de façon toute générale que l'obligation de réparer le préjudice soit répartie entre le titulaire de la clé privée,

l'autorité de certification, le destinataire de l'information signée numériquement (le plus souvent la partie lésée) ou encore une personne totalement étrangère au système d'infrastructure à clé publique qui se serait appropriée la clé privée.
Dans le cadre d'une infrastructure à clé publique, les failles les plus importantes en matière de sécurité dépendent du soin apporté au maintien du caractère confidentiel de la clé privée.
C'est ce que rappelle l'art. 16, en précisant que „les fournisseurs de services de certification reconnus ne peuvent pas conserver de copie des clés privées de leurs clients“ et que „les titulaires d'une clé privée doivent la conserver de manière a prévenir toute utilisation abusive par un tiers. Ils prennent a cet effet les mesures qu'exigent les circonstances“. Par ailleurs, à teneur de l'art. 10 al. 2, les fournisseurs de services de certification reconnus „doivent informer leurs clients des conséquences de la divulgation ou de la perte de leur clé privée, au plus tard lors de la délivrance des certificats électroniques. Ils doivent leur indiquer les mesures appropriées pour maintenir leur clé privée secrète“.

economiesuisse Für die Verbreitung der elektronischen Signatur ist entscheidend, dass sich die Vertragspartner auf sie verlassen dürfen. Die notwendigen privaten Schlüssel können weitergegeben oder allenfalls missbraucht werden – gleich wie eine handschriftliche Unterschrift gefälscht werden kann.
Angesichts der Bedeutung der zu übenden Sorgfalt im Umgang mit dem privaten Schlüssel sind wir der Meinung, dass die Bestimmung in Abs. 2 näher konkretisiert werden sollte. Dies würde sodann die Rechtssicherheit massiv erhöhen. Laut Erläuterungen steht die Bestimmung von Art. 16 auch in engem Zusammenhang mit jenen in Art. 10 Abs. 2, d.h. der Aufklärungspflicht der Zertifizierungsstelle. Abs. 2 von Art. 16 sollte deshalb neu wie folgt lauten: *„[2]Die Inhaber und Inhaberinnen privater Signaturschlüssel müssen diese so aufbewahren, dass sie tatsächlich nur einmal bestehen und eine Verwendung durch unbefugte Drittpersonen ausgeschlossen werden kann. Sie treffen hierzu alle nach den Umständen zumutbaren Vorkehrungen, so insbesondere die in den Ausführungsvorschriften näher spezifizierten und die von den Anbietern von Zertifizierungsdiensten empfohlenen. „*

FGSec Zu Abs. 2: Wir empfehlen: „*mit hoher Wahrscheinlichkeit* ausgeschlossen werden kann."

Der Begriff „ausgeschlossen“ ist nicht zufriedenstellend, und der Begleitbericht geht nicht in genügendem Masse auf die einzelnen Gefährdungen ein. Das Problem ist nicht, sein „Leben zu riskieren", aber die Unterwanderung der Signaturgeräte durch Trojanische Pferde und andere Malware. Keine der momentan verbreiteten Plattformen, und keines der erschwinglichen Geräte, können momentan einer Unterwanderung widerstehen. Ein trojanisches Pferd könnte beispielsweise eine Kopie des privaten Schlüssels, welche auf dem Harddisk des Nutzers gespeichert ist, zum Angreifer senden, oder den privaten Schlüssel verwenden, um ein anderes Dokument zu unterzeichnen, als der Nutzer legitimiert (gesehen) hat, auch wenn der Schlüssel auf einer Smartcard gespeichert ist.

Wir können die Grösse des aus dieser Unterwanderung entstehenden Schadens nicht abschätzen. Kreditkartenfirmen akzeptieren seit Jahren einen gewissen Prozentsatz betrügerischer Transaktionen als Teil ihrer Geschäftstätigkeit, ebenso wie ein Einzelhändler unerklärliche Bestandesrückgänge akzeptiert. Es könnte aber auch katastrophale Ausmasse annehmen, wenn beispielsweise ein verbreiteter E-Mail-Client als sichere Signaturerstellungseinheit

akzeptiert wird und eine Schad-Software dieses System gezielt und verbreitet attackiert.

Es muss definiert werden, was „zumutbar" ist.

FHZ Es wäre sinnvoll, im Gesetz oder auf Verordnungsstufe exemplarisch zu regeln, welche Vorkehrungen zumutbar sind. In VDG 9 beispielsweise sind auch konkrete Massnahmen/Mittel vorgeschlagen, die zur Erfüllung von Datensicherheit in Betracht gezogen werden sollten.

FRC Deuxième phrase : Ils prennent à cet effet les mesures qu'exigent les circonstances.

A rajouter : *„Les fournisseurs de services de certification reconnus leur proposent des mesures concrètes pour prévenir toute utilisation abusive par un tiers. Ils sont tenus de les adapter aux développements techniques nouveaux. Le consommateur est tenu de confirmer qu'il en a pris connaissance".*

La formulation „les mesures qu'exigent les circonstances" est vraiment très vague. Les circonstances changent précisément très vite dans ce domaine et ce qui est sûr aujourd'hui peut très bien ne plus l'être demain, en raison de hackers astucieux. Comme ils ne disposent pas de connaissances techniques approfondies, les consommateurs doivent pouvoir se fier aux mesures de sécurité que leur indiquent régulièrement les fournisseurs de service au fur et à mesure de l'affinement de mesures de sécurité.

FSP Nous constatons que la question de la responsabilité découlant de l'utilisation abusive de clés privées est réglée à l'art. 16.

La lecture attentive du rapport explicatif ne nous permet pas de savoir de quelle façon concrète une telle réglementation sera appliquée. Cependant, il nous apparaît déjà clairement que le système proposé soulèvera d'insolubles problèmes de preuve.

Dans le domaine de la responsabilité liée à l'utilisation des clés privées, le manque de clarté de la loi entraînera à coup sûr des procédures judiciaires ardues et coûteuses.

Jeune Barreau vaudois Le projet ne prévoit une responsabilité qu'en cas de préjudice résultant de la confiance indûment placée dans une signature électronique reposant sur un certificat dont la vérification n'a pas fait apparaître le caractère frauduleux. Sur cette base, le contenu du message transmis est faussement attribué au titulaire de la clé privée indiqué sur le certificat, alors que cette personne n'existe pas ou n'est pas celle qui a signé le message en question.

Dans le cadre d'une infrastructure à clé publique, les failles les plus importantes en matière de sécurité dépendent du soin apporté au maintien du caractère confidentiel de la clé privée.

C'est ce que rappelle l'art. 16, en précisant que „les fournisseurs de services de certification reconnus ne peuvent pas conserver de copie des clés privées de leurs clients" et que „les titulaires d'une clé privée doivent la conserver de manière a prévenir toute utilisation abusive par un tiers. Ils prennent à cet effet les mesures qu'exigent les circonstances". Par ailleurs, à teneur de l'art. 10 al. 2, les fournisseurs de services de certification reconnus „doivent informer leurs clients des conséquences de la divulgation ou de la perte de leur clé privée, au plus tard lors de la délivrance des certificats électroniques. Ils doivent leur indiquer les mesures appropriées pour maintenir leur clé privée secrète".

kf Wer legt im Ernstfall die richtigen Vorkehrungen fest? Diese Vorschrift ist zu unbestimmt. Der Inhaber des privaten Signaturschlüssels haftet ohne klare Kenntnis seiner Pflichten. Diese müssen von den Anbietern oder in einer Verordnung abschliessend vorgeschrieben werden.

Muster/Sury Die Wortwahl „zumutbar“ in Abs. 2 lässt einen breiten „juristischen“ Interpretationsspielraum offen, ist aber der Rechtssicherheit abträglich. Eine genauere Formulierung der zu erfüllenden technischen Massnahmen per Gesetz oder Verordnung ist wünschenswert, insbesondere weil mit diesem Rechtssatz eine Haftungsbefreiung ermöglicht wird (s. Art. 17 Abs. 3).

Rosenthal Vgl. zu Art. 17 / Cf. ad art. 17 / Cfr. ad art. 17.

SBV Il est impératif que le titulaire de la clé privée prenne toutes les mesures en son pouvoir pour tenir sa clé privée secrète. A cet égard, l'obligation de diligence incombant au titulaire devrait être précisée dans l'ordonnance ou dans les dispositions d'exécution. La référence, dans la loi, aux „mesures qu'exigent les circonstances“ nous paraît, à cet égard, insuffisante. Le renvoi à l'art. 10 al. 2 ne permet pas non plus de clarifier cette question, cela en particulier lorsque le fournisseur de services de certification n'a pas lui-même contribué à la génération des clés (voir à ce sujet notre commentaire ad art. 10).

Nous proposons, à cet effet, de compléter comme suit l'art. 16 al. 2:

„Les titulaires d'une clé privée doivent la conserver de manière *à ce qu'elle n'existe qu'en un seul exemplaire* et à en prévenir toute utilisation abusive par un tiers. Ils prennent à cet effet les mesures qu'exigent les circonstances *et en particulier celles énoncées dans les prescriptions d'exécution*“.

„Die Inhaber und Inhaberinnen privater Signaturschlüssel müssen diese so aufbewahren, dass *sie tatsächlich nur einmal bestehen und* eine Verwendung durch unbefugte Drittpersonen ausgeschlossen werden kann. Sie treffen hierzu alle nach den Umständen zumutbaren Vorkehrungen**,** *so insbesondere die in den Ausführungsvorschriften näher spezifizierten*.“

SIK Vgl. zu art. 17 / Cf. ad art. 17 / Cfr. ad art. 17.

SVV Nebst der Gleichstellung der elektronischen Signatur mit der handschriftlichen Unterschrift und den damit verbundenen Problemen des VVG, standen in der Versicherungsbranche insbesondere die Haftungsbestimmungen im Fokus. Die Haftungssituation kann in unseren Augen entscheidend zur Verbreitung der anerkannten elektronischen Signatur beitragen. Wenn auch verständlich auf Grund der eingeschränkten Thematik des BGES, ist insofern zu bedauern, dass das Gesetz nur die Haftungsproblematik der anerkannten Signaturen und nicht aller elektronischen Signaturen anspricht.

Im Rahmen des Meinungsbildungsprozesses innerhalb der Privatassekuranz bildeten die Haftungsbestimmungen in den Art. 16 bis 19 das zentrale Thema. Es steht ausser Frage, dass diese Bestimmungen einen entscheidenden Einfluss auf die Verbreitung der elektronischen Signatur haben werden, denn bei einem Grossteil aller Verträge, die über das Internet abgewickelt werden, ist die Schriftlichkeit kein konstitutives Erfordernis und mithin eine anerkannte Signatur keine Voraussetzung um Verträge online abzuwickeln. Im Vordergrund steht in der Mehrzahl der Fälle die Frage der Identifikation. Wird die Haftung zu einseitig dem Dienstleistungsanbieter auferlegt, wird dieser versucht sein, ein System ohne anerkannte Signatur zu propagieren, da er die Haftungsfragen dann individuell vertraglich festhalten kann. Andererseits wird ein zu strenges Haftungsregime den Benutzer davon abhalten, sich einer elektronischen Signatur zu bedienen. Schliesslich wird auch der Zertifizierungsdienstanbieter an einer möglichst engen Begrenzung seiner Haftung interessiert sein, da sein Produkt ansonsten viel zu teuer zu stehen kommt. In diesem Spannungsverhältnis gilt es, einen goldenen Mittelweg zu finden.

Andere Verfahren wie bspw. biometrische vorbehalten, wird die elektronische Signatur im Vergleich zur handschriftlichen beliebig übertragbar sein. Nebst all

den Chancen, die sich dadurch eröffnen, birgt dieser Umstand auch Gefahren in sich. So muss der Anbieter einer Dienstleistung davon ausgehen können, dass ihm die Person, die sich aus dem öffentlichen Schlüssel ergibt, auch tatsächlich als Vertragspartner gegenüber steht.
Dieser speziellen Situation wird in Art. 17 Rechnung getragen, indem der Vertrag auch bei einem Fremdeinsatz des privaten Signaturschlüssels grundsätzlich zustande kommt, es sei denn, der Inhaber des privaten Schlüssels könne beweisen, die Signatur sei ohne seinen Willen zum Einsatz gelangt. Gelingt dieser Beweis, haftet der Inhaber des Schlüssels immer noch für den Vertrauensschaden, sofern er nicht belegen kann, seinen Sorgfaltspflichten nachgekommen zu sein.
Diese Haftungssituation wurde innerhalb der Privatassekuranz als ausgewogen taxiert. Damit ein von Rechtssicherheit geprägtes Umfeld allerdings entstehen kann, versteht sich, dass die Gerichte das Niveau des Beweises im Vergleich zur blossen Behauptung, der Schlüssel sei ohne Willen zum Einsatz gelangt, entscheidend höher ansetzen. Ansonsten wäre dem Inhaber einer Signatur allzu leicht anheimgestellt, sich von seiner vertraglichen Bindung loszusagen, auch wenn er je nach Umstand den Vertrauensschaden immer noch zu tragen hätte. Nicht zuletzt diese Befürchtung hat dazu beigetragen, dass die Privatversicherer mit anderen Lösungen geliebäugelt haben. Im Vordergrund standen dabei Varianten, bei denen die mangelnde Vollmacht durch den guten Glauben des Anbieters von Waren oder Dienstleistungen geheilt würde, ausser der Inhaber der Signatur könne beweisen, dass er all seinen Sorgfaltspflichten bezüglich der Geheimhaltung nachgekommen ist. Ähnliche Lösungen werden von anderen Kreisen der Wirtschaft propagiert. Wenn auch einiges für einen erhöhten Schutz des Dienstanbieters spricht, haben wir uns dennoch entschieden, grundsätzlich für das in Art. 16 ff. entworfene Konstrukt zu plädieren.
Abs. 2: „Die Inhaber und Inhaberinnen privater Signaturschlüssel müssen diese so aufbewahren, dass eine Verwendung durch unbefugte Drittpersonen ausgeschlossen werden kann. Sie treffen hierzu alle nach den Umständen zumutbaren Vorkehrungen. *Die einzuhaltenden Sorgfaltspflichten richten sich nach Art. 10 Abs. 2 BGES“.*
Begründung: Art. 16 Abs. 2 steht in einem engen Konnex zu Art. 10 Abs. 2. Wie bereits oben erwähnt, kommt den Sorgfaltspflichten bei der Geheimhaltung des privaten Schlüssels eine hohe Bedeutung zu. Die Wendung in Art. 16 Abs. 2, wonach die Inhaber privater Signaturschlüssel „alle nach den Umständen zumutbaren Vorkehrungen zu treffen haben“, dass der Schlüssel nicht unbefugt durch Dritte verwendet wird, liefert den notwendigen Nachdruck. Damit der Vorschrift auch faktisch Rechnung getragen wird, ist insbesondere die Einhaltung der Sorgfaltspflichten in Art. 10 Abs. 2 notwendig. Um das Mass der Vorkehrungen zu konkretisieren, beantragen wir einen entsprechenden Verweis in Art. 16 Abs. 2.

SWICO Der ganze Abschnitt bedarf der Revision. Wir sind der Ansicht, dass an dieser Stelle die Sphärentheorie zur Anwendung kommen sollte. Diese bedeutet einerseits, dass der Verantwortungsbereich der Parteien klar zu regeln ist, andererseits die Sorgfaltspflicht genau beschrieben wird. Die Artikel sind deshalb wie folgt zu gliedern:

1. Verantwortungsbereich
2. Umschreibung der Sorgfaltspflicht
3. Konsequenzen bei einer Verletzung der Sorgfaltspflicht

Heute fehlt im Entwurf eine Regelung zu Verantwortlichkeit der Relying Party. Die Problematik bei Signatursystemen besteht nämlich darin, dass Zertifikate bereits abgelaufen sein können und dies vom gutgläubigen Anwender nicht geprüft bzw. übersehen wurde. Man muss dem Anwender die Verpflichtung auferlegen, die Gültigkeit des Zertifikats beim Abschluss eines Rechtsgeschäftes zwingend zu überprüfen. Im vorliegenden Gesetzesentwurf besteht zwar eine Verpflichtung der Anbieter von Zertifizierungsdiensten, diese Verzeichnisse anzubieten (Art. 12), jedoch keine Verpflichtung der Relying Parties, diese tatsächlich auch zu prüfen. Hier kann man – u.a. aus Kostengründen - zu Recht diskutieren, ob man dies zur Verpflichtung machen sollte; u.E. sollte dies auf jeden Fall vorgesehen werden. Damit erreicht man eine verbesserte Automatisierung der Abläufe (kostenrelevant), aber vor allem auch eine höhere Akzeptanz durch die Anwender.

Es macht wenig Sinn, die Verantwortlichkeit dafür der Anbieterin von Zertifizierungsdiensten zu übertragen, da diese hier keine Kontrollmöglichkeit hat.

Abs. 2 sollte nach dem Leitbild der Sphärentheorie und der praktischen Risikosituation eine sachgerechte, nähere Spezifikation erfolgen. Laut Erläuterungen soll diese Bestimmung in engem Zusammenhang mit Art. 10 Abs. 2 stehen, d.h. der Aufklärungspflicht der Zertifizierungsstelle. Dies würde die Qualität dieser neuen Systeme und damit auch die Zuordnung der Risikotragung praxisgerechter machen.

So sollte u.a. festgehalten werden, dass der Inhaber (i)den Verlust umgehend zu melden bzw. den Schlüssel und das Zertifikat sperren zu lassen hat und (ii)den privaten Signaturschlüssel strikte geheim zu halten hat und keinesfalls einer anderen Person überlassen werden darf. Abs. 2 sollte somit lauten: „Die Inhaber und Inhaberinnen privater Signaturschlüssel müssen diese so aufbewahren, *dass sie tatsächlich nur einmal bestehen und* eine Verwendung durch unbefugte Drittpersonen ausgeschlossen werden kann. Sie treffen hierzu alle nach den Umständen zumutbaren Vorkehrungen*, so insbesondere die im Gesetz und in den Ausführungsvorschriften näher spezifizierten*."

Organisationen / Organisations / Organizzazioni

ISACA Vgl. zu Art. 10 / Cf. ad art. 10 / Cfr. ad art. 10.

321.17 Art. 17

Kantone / Cantons / Cantoni

AI Als problematisch wird die Beweispflicht der Person, von welcher der private Signaturschlüssel verwendet wurde (Missbrauch / ohne ihren Willen), erachtet. In Art. 17 sollte zumindest eine angemessene Unterstützungspflicht des Anbieters stipuliert werden.

BL Es sollte geprüft werden, ob Art. 17 mit folgender Regelung zu ergänzen ist: An Stellen, wo der private Schlüssel eingegeben werden kann, ist es untersagt, Aufzeichnungsgeräte zu installieren, die eine Rekonstruktion des Signaturschlüssels, der Passphrase etc. ermöglichen. Damit soll verhindert werden, dass Kameras oder andere elektronische Aufzeichnungsgeräte installiert werden, die eine Rekonstruktion des Signaturschlüssels, der Passphrase etc. ermöglichen.

Vgl. auch zu Art. 10 / Cf. également ad art. 10 / Cfr. anche ad art. 10.

GE Dans une autre perspective, l'articulation entre l'al. 1 et l'al. 3 de l'art. 17 n'est pas évidente. Celui qui échoue dans la preuve que sa clé privée a été utilisée sans son consentement (al. 1) est-il néanmoins fondé à se libérer de sa res-

ponsabilité en démontrant qu'il a adopté les mesures exigées par les circonstances pour prévenir toute utilisation abusive par un tiers (al. 3) ?

JU Le système de responsabilité mis en place implique une prise de risque concrète pour celui qui se fie à un certificat valable, dans la mesure où les conditions mises à la libération de responsabilité pour le titulaire de la clé privée lui échappent dans une très large mesure. En particulier, il n'a aucune maîtrise sur les précautions prises pour éviter un emploi abusif d'une clé.

NE L'al. 3 devrait être complété de la manière suivante: „ ... prévu à l'art. 16 al. 2, *ou s'il a respecté les mesures appropriées établies par le fournisseur de service pour maintenir sa clé privée secrète (art. 10 al. 2)*."
En effet, nous ne voyons pas la raison pour laquelle le titulaire d'une clé privée qui aurait respecté scrupuleusement les directives de sécurité de son fournisseur de services ne serait pas libéré de sa responsabilité de ce seul chef.

SG Den im Zusammenhang mit dem privatrechtlichen Vertragsabschluss vorgeschlagenen Haftungsregelungen ist insofern zuzustimmen, als sie vom Grundsatz ausgehen, dass auch in Zukunft die Inhaberin und der Inhaber eines privaten Signaturschlüssels nur aus Vertrag haftet, wenn sie bzw. er diesem zustimmt. Die in Art. 17 Abs. 1 vorgesehene Umkehr der Beweislast erachten wir jedoch – je nach der zum Einsatz kommenden Technik – als problematisch. Sie kann die Benutzerinnen und Benutzer überfordern, da sie beim Einsatz der elektronischen Signatur den Risiken aller weiteren von ihnen nicht direkt beeinflussbaren Systeme ausgeliefert sind. In diesem Sinn dürfen die Anforderungen an den Beweis nicht zu hoch gesteckt werden bzw. die Vorkehrungen zur sicheren Aufbewahrung des Signaturschlüssels den Rahmen des Zumutbaren nicht überschreiten. Dem ist bei der Ausgestaltung der entsprechenden Verordnungsbestimmungen Rechnung zu tragen.
Wir beantragen, in Art. 17 den jetzigen Abs. 1 als Abs. 3 vorzusehen.
Begründung: Der eigentliche - im Randtitel bezeichnete - Regelungsgehalt der Bestimmung findet sich in Abs. 2. Insofern sind Art. 17 und 18 systematisch gleich aufzubauen.

TG Zu begrüssen ist die in Art. 17 vorgeschlagene Regelung der Haftung des Inhabers des privaten Signaturschlüssels. Richtig ist, dass diejenige Person, welche behauptet, ihr privater Signaturschlüssel sei ohne ihren Willen zum Einsatz gelangt, hierfür beweispflichtig wird. Als sinnvoll erscheint, mit dem Hinweis auf die Bestimmungen des Obligationenrechts über die Stellvertretung ohne Ermächtigung auf bewährte Regelungen zurückzugreifen.

VD S'agissant des questions de responsabilité, l'on devrait opérer une distinction entre les problèmes directement liés à la certification des signatures électroniques et ceux qui relèvent des principes généraux du droit des obligations. Selon le rapport explicatif, les premiers impliquent l'existence d'une responsabilité causale (page 22) alors que les seconds relèvent d'une responsabilité en cas de conduite illicite ou fautive (page 21).
Par ailleurs, les questions plus particulièrement liées aux relations entre le titulaire d'une clé privée et ses partenaires contractuels mériteraient d'être traitées en même temps que les autres modifications du Code des obligations envisagées dans le cadre de la loi sur le commerce électronique.

ZG Für die Einführung der elektronischen Signatur erscheint uns die Haftungsregelung von Art. 17 problematisch. Wenn eine Person, die behauptet, ihr privater Signaturschlüssel sei ohne ihren Willen zum Einsatz gelangt, dafür ausnahmslos beweispflichtig ist, werden sich viele potentielle Interessenten die Anwendung der neuen Technik wohl grundlegend überlegen. Dem durchschnitt-

lichen privaten Nutzer der digitalen Unterschrift wird das notwendige Fachwissen fehlen, um seinen Computer so einbruchssicher zu betreiben, dass die digitale Unterschrift nicht entwendet werden kann. Unseres Erachtens darf die Einführung der digitalen Signatur im Geschäfts- und Behördenverkehr nicht durch eine derart rigorose Haftung des Schlüsselinhabers behindert werden.

Parteien / Partis / Partiti

Jungfreisinnige Die digitale Signatur ist keine persönliche Unterschrift, wie es eine Unterschrift von Hand ist. Anders als letztere ist eine digitale Signatur faktisch übertragbar, weil alles was es zu deren Erzeugung braucht – der private Schlüssel – eine Zahlenkombination ist. Der Inhaber wird diesen zwar im eigenen Interesse geheim halten. Tut er dies aber nicht und wird der Schlüssel von einem Dritten benutzt – was der Empfänger der Signatur nicht ansieht -, liegt plötzlich ein Fall von Stellvertretung vor, wie ihn das Obligationenrecht schon lange kennt. Das soll wiederum zur Folge haben, dass der Inhaber einer anerkannten Signatur nur dann für eine mit seiner Signatur vorgesehenen Vertragserklärung einstehen muss, wenn er dieser vorgängig oder nachträglich zugestimmt hat. Wird also die Signatur einer Person nachweislich ohne deren Zustimmung für Vertragserklärung gebraucht, wird sie nicht verpflichtet; allenfalls trifft sie und den wahren Signierer eine Haftung, doch der Vertrag ist nicht zustande gekommen. Bei einer vom Signaturinhaber selbst unterzeichneten Vertragserklärung auf Papier gäbe es diese Rückzugmöglichkeit nicht, weil eine eigenhändige Unterschrift einer Person naturgemäss nicht durch Dritte möglich ist (siehe D. Rosenthal, Digitale Identitäten, NZZ 26. Januar 2001).

Schliesslich muss der Signaturinhaber im Streitfall beweisen, dass die Signatur ohne seinen Willen gebraucht wurde. Es ist aber unklar, wie ein solcher Beweis erbracht werden kann und wie diese Regelung in das bestehende Vertragsrecht passt.

Wir möchten deshalb, dass der Bundesrat diese Problematik nochmals durchdenkt und Lösungsvorschläge unterbreitet.

Die Problematik der Haftung sollte nochmals überdenkt werden. Es muss alles getan werden, um das Vertrauen der Bevölkerung zu gewinnen. Dem Bürger muss deshalb ein Weg aufgezeigt werden, wie er sich bei unverschuldeten Schaden durch die digitale Signatur schützen kann.

PLS Compte tenu du renversement du fardeau de la preuve, le titulaire de la clé privée devrait répondre de l'ensemble des événements qui se produisent dans sa sphère d'influence. L'étendue de la preuve pourrait être précisée comme suit : ni le titulaire de la clé privée ni un fondé de procuration désigné par lui ou encore une personne de son entourage n'ont, dans un cas donné, utilisé la clé; le titulaire a conservé la clé - de même que le matériel informatique nécessaire à son utilisation - avec la diligence requise.

Organisationen / Organisations / Organizzazioni

Briner In Art. 17 Abs. 3 wird die Haftung geregelt und heisst es anschliessend, dass „im übrigen" die Art. 38/39 OR gelten. Diese beiden Artikel regeln bekanntlich weit mehr als nur Haftung, und das sollte auch so bleiben, auch wenn digitale Signaturen im Spiel sind.

Vgl. auch zu Art. 16 / Cf. également ad art. 16 / Cfr. anche ad art. 16.

Clusis L'art. 17 est entièrement consacré à la responsabilité du titulaire de la clé privée de signature. Son articulation n'est pas très claire. Il semble que le principe soit exprimé à l'art. 17 al. 2, en vertu duquel „le titulaire d'une clé privée

répond envers les tiers des dommages que ces derniers ont subis parce qu'ils se sont fiés à un certificat valable, délivré par un fournisseur de services de certification reconnu“ et que l'exception soit contenue à l'al. 3 qui prévoit que „le titulaire de la clé privée est libéré de sa responsabilité s'il a adopté les mesures prévues a l'art. 16 al. 2. Au surplus, les dispositions du Code des obligations sur la représentation sans pouvoir (art. 38 et 39) sont applicables“.

Notons d'abord que la référence aux art. 38 et 39 du Code des obligations paraissait superflue dans la mesure où ils étaient de toute façon applicables.

Le système mis en place est donc celui d'une responsabilité du titulaire d'une clé privée pour les dommages découlant d'une vérification d'un certificat valable, à moins que le titulaire de cette même clé privée ne prouve qu'il a respecté son obligation, contenue à l'art. 16 al. 2 de conserver „sa clé privée de manière a en prévenir toute utilisation abusive par un tiers, en prenant a cet effet les mesures qu'exigent les circonstances“.

Une telle formulation est cependant problématique, dans la mesure où une simple référence aux „mesures qu'exigent les circonstances“ est évidemment source de litige et d'ambiguïté. Elles pourraient en particulier dépendre de l'importance du contenu des informations signées.

Par ailleurs, l'utilité de l'art. 17 al. 1 n'est pas forcément évidente. On rappelle que cet alinéa prévoit qu'il „appartient à celui qui affirme que sa clé privée a été utilisée sans son consentement d'en apporter la preuve“. On peut tout d'abord se demander s'il s'agit réellement d'un renversement du fardeau de la preuve, comme le prétend le rapport explicatif (ch. 210.072). Surtout, il faudrait s'interroger sur les conséquences du succès ou de l'échec de cette preuve sur l'éventuelle responsabilité du titulaire de la clé privée, qui est la question centrale. A supposer par exemple que le titulaire de la clé privée puisse apporter la preuve que celle-ci a été utilisée sans son consentement, mais que cette utilisation abusive a été rendue possible par sa négligence dans le maintien du caractère secret de sa clé privée, le motif libératoire de l'al. 3 ne serait pas invocable et sa responsabilité serait engagée en vertu de l'al. 2. A l'inverse, si le titulaire de la clé privée échoue dans sa preuve d'une utilisation sans son consentement de cette clé privée, il pourrait néanmoins être libéré de toute responsabilité, en vertu de l'al. 3, s'il a adopté les mesures qu'exigeaient les circonstances.

A relever enfin que, selon le rapport explicatif (ch. 210.072), ces dispositions sont de nature dispositive, si bien que la véritable étendue de la responsabilité du titulaire de la clé privée sera déterminée par le contenu du contrat le liant avec le destinataire d'une telle transmission. Il n’est d'ailleurs pas certain que celui-ci soit entièrement protégé, notamment dans une situation où les parties ont un pouvoir de négociation inégal.

FRC A compléter: „Il appartient à celui qui affirme que sa clé privée a été utilisée sans son consentement d'en apporter la preuve. *Le dispositif d'horodatage (Zeitstempel) constitue un moyen de preuve“.* Nous constatons qu'il est extrêmement difficile pour le consommateur de prouver que sa clé privée a été utilisée sans son consentement. Le consommateur rencontre les mêmes difficultés pour les cartes de crédit. A cela s'ajoute qu'il peut se passer plusieurs semaines avant qu'il remarque que sa clé privée a été volée. Les conséquences financières peuvent donc être très lourdes pour lui. Nous n'acceptons cet article que sous réserve d'un nouvel al. 3 inscrit dans la loi :

„Le titulaire de la clé privée est libéré de sa responsabilité s'il a adopté les mesures prévues à l'art. 16, al. 2, consignées dans une check-list de mesures de

sécurité mise régulièrement à jour par le fournisseur de services de certification reconnus".

FRI Les articles relatifs notamment à la délivrance et l'annulation des certificats électroniques décrivent avec pertinence les obligations des fournisseurs de services de certification. Il s'agira dès lors de faire respecter ce quasi „code de conduite" dont dépend la fiabilité du système tout entier.

ISACA Vgl. zu Art. 10 / Cf. ad art. 10 / Cfr. ad art. 10.

economiesuisse Im selben Sinne wie / Dans le même sens que / Nello stesso senso che SWICO.

FGSec Zu Abs. 1: „Beweispflichtig" zu sein, ist kritisch, da eine Unterwanderungsgefahr auf jeder Plattform besteht. Es besteht niemals eine Gewähr für die Grundvoraussetzung „What You See Is What You Sign".

Zu Abs. 3: Art. 16 definiert keine Vorkehrungen, sondern bezieht sich nur auf das „Zumutbare".

Jeune Barreau vaudois Wie / Comme / Come Clusis.

kf Die Aussagen unter Absatz 3 mit dem Hinweis auf Art. 26 Abs. 2 müssen zwingend erhalten bleiben und deshalb ist die Festlegung, was unter den „richtigen" Vorkehrungen gemeint ist, für uns zentral.

KPMG Wir sind der Ansicht, dass die charakteristischen Merkmale einer Unterschrift nicht nur mit der handschriftlichen, sondern auch anhand der elektronischen Unterschrift erfüllt werden können. Wichtig scheint uns deshalb, dass die Rechtsgrundlagen zur digitalen Signatur sowohl in formeller als auch in materieller Hinsicht Voraussetzungen schaffen, damit der Benutzer in Zukunft aus zwei rechtlich gleichwertigen Unterschriftsarten, nämlich der elektronischen und der handschriftlichen, wählen kann. Wir schlagen deshalb vor, auf spezielle Haftungsnormen zu verzichten und die elektronische Signatur soweit möglich in das geltende Rechtssystem einzubetten. Damit würde auch eine bessere Übereinstimmung mit den entsprechenden - soweit diese heute bereits bekannt sind - ausländischen Normen erreicht.

Wie bereits einführend erwähnt, sind wir der Meinung, dass für „digitale Signaturen" nur dort neue Rechtsgrundlagen geschaffen werden sollen, wo aus technischen, betrieblichen und rechtlichen Erwägungen neue Rechtsnormen tatsächlich auch erforderlich sind. Grundsätzlich sollten die geltenden Normen sowie die herrschende Lehre und Rechtsprechung auch für digitale Signaturen übernommen und für alle Unterschriftsformen gleichermassen weiterentwickelt werden. Bevor wir uns deshalb mit der Vertragsentstehung im Zusammenhang mit der digitalen Signatur näher auseinandersetzen, möchten wir die geltende Rechtslage zur handschriftlichen Unterschrift analysieren, um uns anschliessend auf die Unterschiede der beiden Unterschriftsarten konzentrieren zu können.

Zum Abschluss eines Vertrags bedarf es der übereinstimmenden gegenseitigen Willensäusserung der beteiligten Parteien (Art. 1 Abs. 1 OR), wobei die Willensäusserungen ausdrücklich oder stillschweigend erfolgen (Art. 1 Abs. 2 OR) können.

Dieses Erfordernis einer gültigen Willenserklärung bedeutet, dass kein Vertrag zu Stande kommt, sofern überhaupt keine ursächliche Beziehung zwischen einem Verhalten des vermeintlich Erklärenden und dem falschen Konsensbewusstsein des vermeintlichen Empfängers gegeben ist (SCHÖNENBERGER Wilhelm, JÄGGI Peter, Kommentar zum Schweizerischen Zivilgesetzbuch, Teilband V 1a, Zürich 1973, Art. 1 N 424). Damit wird der Erklärungsempfänger auch dann nicht geschützt, wenn er gutgläubig auf die Gültigkeit der Erklärung ver-

traute und auch vertrauen konnte (Siehe auch BGE 88 II 422 E.2c mit Hinweis auf VON THUR/SIEGWART OR II § 96 Ziff. V. S. 811f.).
*Beispiel: A schliesst anhand einer gefälschten Vollmacht mit B zu Lasten des C einen Kaufvertrag ab. C weiss vom Ansinnen des A nichts und will auch keinen Vertrag abschliessen. Zwischen C und B kommt kein Vertrag zu Stande. C muss sich den Vertrag weder anrechnen lassen, noch muss er B Schadenersatz leisten. B kann sich höchstens an A schadlos halten (*Ein Vertrag zwischen A und B kommt nur zu Stande, wenn B einer Änderung der Vertragspartei zustimmt*).*
Besteht jedoch eine, wie auch immer geartete Kausalbeziehung zwischen der Handlung des Erklärenden (oder der Person, deren Handlungen ihm aufgrund einer gesetzlichen oder vertraglichen Rechtsgrundlage angerechnet werden) und des falschen Erklärungsscheins, so entsteht eine Haftung für den falschen Erklärungsschein. Diese Haftung richtet sich nach den Regeln des allgemeinen Haftpflichtrechts (Art. 41ff. OR). Es geht hier deshalb nicht um die Zurechnung von Vertragswirkungen, sondern um die Leistung von Schadenersatz für das (unbeabsichtigte) Verhalten, das den Rechtsschein auslöste. Wer aufgrund der Umstände mit einem Missbrauch seiner Erklärungshandlung rechnen musste und die zur Abwendung der Gefahr erforderlichen und zumutbaren Abwehrmassnahmen nicht getroffen hat, trägt an den daraus entstehenden Schäden ein Mitverschulden.
Beispiel: A füllt ein Formular, das B im Geschäftsverkehr verwendet, so aus (z.B. durch Fälschung der Unterschrift), dass es als Erklärung des B (oder eines Vertreters des B) erscheint.
Beispiel: A bewahrt blanko unterzeichnetes Briefpapier an einem jedermann zugänglichen Ort auf. B bemächtigt sich der Blankourkunde und missbraucht diese für eine Verpflichtungserklärung des A gegenüber dem B.
Beispiel: A unterzeichnet den Vertrag mit B, hält ihn aber in der Schublade zurück und will über die Absendung nochmals nachdenken. B entnimmt den Vertrag der Schublade und verschickt ihn.
In all diesen Fällen ist kein Vertrag zu Stande gekommen. Ein (Mit-)Verschulden des Unterzeichneten am Rechtsschein des Vertragsabschlusses ist jedoch zu bejahen, weshalb eine Schadensübernahme nach Abwägen der konkreten Umstände vorzusehen ist.
In einzelnen (wenigen) Fällen (eine entsprechende Sorgfaltspflicht kennt Art. 1132 OR für gefälschte Checks [siehe dazu auch BGE 24 II 588, 122 III 26, 122 III 373 und 122 III 379E. 3b]. Art. 1132 OR ist dispositiver Natur und wird von Banken oft im Rahmen allgemeiner Geschäftsbedingungen soweit gemäss Art. 101 OR zulässig, wegbedungen] gilt eine gesteigerte Haftung und geht die Verpflichtung des Erklärenden sogar soweit, dass er sich die Folgen seiner Scheinerklärung voll anrechnen lassen muss. Zum Blankettmissbrauch sagt das Bundesgericht folgendes: „Die Billigkeit gebietet jedoch, in erster Linie den Aussteller das Risiko des Blankettmissbrauchs tragen zu lassen und ihn auf einen Schadenersatzanspruch gegen den Ausfüllenden zu verweisen (VON THUR/SIEGWART OR II S. 152 Note 32). Durch die Ausstellung des Blanketts hat er die Möglichkeit des Missbrauchs erst geschaffen und damit den Rechtsschein veranlasst, dass der von seinem Vertrauensmann weisungswidrig über die Blanko-Unterschrift gesetzte Text der Urkunde seinem Willen entspreche. Er muss sich daher nach den Grundsätzen von Treu und Glauben im Verkehr gegenüber einem gutgläubigen Dritten so behandeln lassen, als ob der so er-

weckte Rechtsschein der wahren Sachlage entspreche“ (siehe dazu auch BGE 88 II 424ff.).
Beispiel: A übergibt ein blanko unterzeichnetes Briefpapier seinem Angestellten X, damit dieser einen Vertrag während seiner Abwesenheit finalisieren und dem Vertragspartner zustellen kann. X missbraucht die Blanko-Unterschrift, indem er damit eine Vollmacht erstellt mit der Anweisung an eine Bank, dem Arbeitnehmer X Geld in bar auszuzahlen.
Die schärfere Haftung rechtfertigt sich hier deshalb, weil der Blankettgeber dem Blankettnehmer eine unterzeichnete Urkunde übergibt; missbraucht der Blankettnehmer diese Urkunde, so hat der Blankettgeber, der schliesslich die Vertrauensperson ausgewählt hat, die entsprechenden Folgen zu tragen und nicht der getäuschte gutgläubige Dritte.
Im Gegensatz zur unterschobenen Erklärung, wo jeder Erklärungswille und damit auch der Geschäftswille des Erklärenden fehlt, äussert hier der Erklärende einen rechtsgeschäftlichen Willen und der Empfänger der Erklärung hat eine Vorstellung dieses erklärten Willens. Anders als beim Konsens stimmen diese Elemente jedoch nicht miteinander überein.
Konsens bedeutet Willensübereinstimmung, d.h. die Übereinstimmung des Willens der Vertragspartner darüber, dass ein Vertrag mit bestimmtem Inhalt ihre rechtliche Beziehung regeln soll. Zum allgemeinen Konsens kommt der Vertragskonsens hinzu, nämlich der Wille, gemäss diesem allgemeinen Konsens (vertrags-)rechtlich auch gebunden sein zu wollen. Fehlt dieser Vertragsabschlusswille, so kommt kein Vertrag zu Stande. Ob ein Vertrag zu Stande gekommen ist, d.h. ob Konsens zwischen den Parteien besteht, beurteilt sich nach allgemein anerkannter Lehre und Rechtsprechung nach dem Vertrauens- bzw. Erklärungsprinzip. Massgebend ist damit der objektive Gehalt, der einer Erklärung entnommen werden kann, d.h. es kommt nicht auf den inneren Willen des Erklärenden an, sondern vielmehr darauf, welches der Sinn seiner Erklärung ist, die diese bei einem redlichen und vernünftigen Empfänger erwekken muss (BUCHER Eugen, Schweizerisches Obligationenrecht, Allgemeiner Teil, Zürich 1988, Seite 122). Kommen Vertragswirkungen nicht durch übereinstimmende Willensäusserungen (natürlicher Konsens) zu Stande, sondern aufgrund des Vertrauensprinzips (d.h. eine Partei durfte die Erklärung der anderen Partei als mit ihrem Willen übereinstimmend verstehen), so liegt normativer Konsens vor, der juristisch dem natürlichen Konsens gleichgestellt wird und damit als übereinstimmende Willenserklärung auch genügt. Dissens bedeutet demzufolge fehlender natürlicher respektive normativer Konsens.
Besteht zwischen den Parteien Dissens, so ist - von Gesetzes wegen - kein Vertrag zu Stande gekommen. Grundsätzlich hat jede Partei einen aus dem Nichtzustandekommen des Vertrags entstandenen Schaden selber zu tragen. Auf der Grundlage der „culpa in contrahendo-Haftung“ ist jedoch eine Schadenersatzzahlung angebracht, sofern eine Vertragspartei den Dissens erkennt, den Vertragspartner darüber jedoch nicht unverzüglich informiert (BUCHER Eugen, a.a.O., Seite 145).
Wird der von der Erklärung abweichende tatsächliche innere Wille im Stadium des Vertragsschlusses nicht berücksichtigt, so kommt er umgekehrt im Rahmen der Anfechtung eines Willensmangels voll zum Zuge. Ein Willensmangel liegt vor, wenn der Vertragswille eines Vertragspartners im weitesten Sinne mangelhaft gebildet wurde. Im Gegensatz zum Dissens führen Willensmängel nicht per se zur Vertragsungültigkeit, sondern sind lediglich vom irrenden Vertragspartner anfechtbar, sofern der Irrtum wesentlich ist (Art. 23 OR).

In der Schweiz steht die Irrtumsanfechtung auf dem Boden der Willenstheorie; damit korrigiert sie wenigstens teilweise die für den Empfänger oft nachteilige Erklärungstheorie bei der Ebene der Vertragsentstehung.
Auf die einzelnen Irrtumstatbestände wird hier - von einer Ausnahme abgesehen - nicht weiter eingegangen. Das Bundesgericht hat die Frage, ob eine Blankourkunde, die gegen den Willen des Unterzeichneten ausgefüllt wird, mittels Erklärungsirrtum angefochten werden kann, mit der Begründung verneint, dass eine Partei, die eine dem Wortlaut des Texts entsprechende Erklärung abgibt, sich dem Inhalt der Erklärung wie er effektiv lautet unterwirft (BGE 88 II 427f. Siehe dazu auch OFTINGER Karl, Die ungelesen unterzeichnete Urkunde und verwandte Tatbestände, in: Ausgewählte Schriften, Zürich 1978, Seite 145ff., insb. Seite 148). Ob der auf die Gültigkeit der Urkunde Vertrauende, Rechtsschutz geniesst oder nicht, wird sich von Fall zu Fall zeigen müssen, je nachdem, ob er Rechtsschutz nach Art. 2 ZGB bzw. Art. 25 Abs. 1 OR verdient. Kannte beispielsweise der Dritte den Missbrauch der Urkunde, verdient er keinen Schutz.
Im vorhergehenden Abschnitt haben wir kurz einzelne Tatbestände im Zusammenhang mit fehlerhaften Willensäusserungen aufgrund der heute geltenden Rechtslage aufgeführt. Nachfolgend geht es uns darum, darzulegen, dass das geltende Recht genügt, um diese „Störungen“ auch beim Gebrauch der digitalen Signaturen rechtlich beheben zu können. Wir sind deshalb der Meinung, dass auf zusätzliche Gesetzesnormen verzichtet werden kann. Dieser Verzicht ist umso wichtiger, als neue Regeln zusätzliche Abgrenzungsschwierigkeiten hervorrufen: Dies dient der Rechtssicherheit nicht. Entgegen oft geäusserten Meinungen und Befürchtungen sind wir überzeugt, dass die elektronische Signatur auch im Zusammenhang mit den Vertragswirkungen der gesetzlichen und gewillkürten eigenhändigen Unterschrift gleichgestellt ist und gleichgestellt werden muss.
Wie in Ziffer 2.2.1 erläutert, ist dann kein Vertrag zu Stande gekommen, wenn keine ursächliche Beziehung zwischen einem Verhalten des Erklärenden und dem falschen Konsensbewusstsein des Empfängers vorliegt. Auch der gutgläubige Empfänger verdient in diesem Fall keinen Schutz.
Beispiel: A schliesst mit B zu Lasten des C einen Kaufvertrag ab, indem er sich des privaten Signaturschlüssels des C behändigt. C weiss vom Ansinnen des A nichts und will auch keinen Vertrag abschliessen. Zwischen C und B kommt kein Vertrag zu Stande. C muss sich den Vertrag weder anrechnen lassen noch muss er B Schadenersatz leisten. B kann sich höchstens an A schadlos halten.
Obwohl dieses Ergebnis grundsätzlich mit den Ausführungen im Begleitbericht zum Entwurf für ein Bundesgesetz über die elektronische Signatur („Bericht 2001“) zu Art. 17 (siehe Seite 22) übereinstimmt, sind wir der Meinung, dass in diesem Abschnitt die einzelnen Teile eines Vertragsabschlusses systematischer aufgearbeitet werden sollten. Die Frage der Stellvertretung stellt sich erst, nachdem eindeutig feststeht, dass eine Willensäusserung dem Vertretenen zuzurechnen ist. Unseres Erachtens sollte im Bericht 2001 stärker auf die allgemeinen Fragen der Vertragsentstehung eingegangen werden. Wird die eigenhändige Unterschrift des angeblich Erklärenden durch einen Dritten gefälscht, so ist die Rechtslage genau gleich, wie wenn er die elektronische Unterschrift eines anderen dazu verwendet, einen Vertrag abzuschliessen. Da, wie in Ziffer 1.2 ausgeführt, die Identifikation des Unterzeichneten zusammen mit einer elektronischen Signatur viel besser nachgewiesen werden kann als bei einer handschriftlichen Unterschrift, ist der Erklärungsempfänger jedoch eher in der

Lage, die Unterschiebung einer Erklärung zu erkennen. Diese Tatsache kann Auswirkungen auf ein eventuelles Mitverschulden haben. Obwohl eine Pflicht, sich im Verzeichnis der elektronischen Zertifikate eintragen zu lassen, fehlt (Art. 12 Abs. 1 E-BGES), ist voraussichtlich die Chance, einen entsprechenden Eintrag zu finden um einiges grösser als unter der bestehenden Rechtslage, gibt es doch heute im Geschäftsverkehr nur selten und im Privatverkehr überhaupt keine Möglichkeit, die handschriftliche Unterschrift mittels eines Unterschriftenverzeichnisses zu überprüfen. Aufgrund dieser Sachlage wäre es eventuell sinnvoll, die Eintragung obligatorisch zu erklären.

Beispiel: (Das Beispiel ist dem D-Entwurf entnommen (Seite 22) *A will die bereits fertiggestellte, z.B. im PC gespeicherte und möglicherweise schon elektronisch signierte Erklärung noch nicht an den Vertragspartner B weiterleiten. Geht nun die Erklärung dem B trotzdem zu, indem bspw. B oder ein Dritter den Sendebefehl aktiviert, so ist die Erklärung nicht willentlich und damit rechtlich nicht abgegeben, weshalb zwischen A und B auch kein Vertrag entsteht. In diesem Fall ist jedoch der Vertrauensschaden zu ersetzen.*

Diese Fallkonstellation entspricht jener von Beispiel 4 hiervor. Die Haftung basiert auch hier wieder auf den allgemeinen Normen des Haftpflichtrechts gemäss Art. 41ff. bzw. Art. 55 OR. Der erforderliche Verschuldensnachweis könnte dadurch erbracht werden, dass der Unterzeichnete nicht die geeigneten Vorkehrungen getroffen hat (bspw. den Einbau von Zugangssperren; separate Aufbewahrung von Chipkarte und PIN-Code), um solchen unbefugten Zugriff zu verhindern.

Wer wissentlich und willentlich einem Dritten seine digitale Signatur zur Verfügung stellt (siehe Beispiel 5), ist mitschuldig, wenn anschliessend diese Unterschrift nicht in seinem Sinn verwendet wird; ihm ist dementsprechend der Inhalt des Dokuments anzurechnen, wobei auch hier ein Mitverschulden dem Empfänger anzurechnen wäre, sofern er den Missbrauch der Unterschrift hätte erkennen können. Dies wäre beispielsweise dann anzunehmen, wenn sich der Inhaber des privaten Schlüssels im Verzeichnis der elektronischen Zertifikate eintragen liess und der Empfänger deshalb den Fehler hätte erkennen können, hätte er das öffentliche Verzeichnis (Art. 12 Abs. 3 E-BGES) konsultiert.

Beispiel: A übergibt seinem Angestellten X seine Chip-Karte und seinen PIN, damit dieser den Vertrag während der Abwesenheit des Unterzeichneten finalisieren, elektronisch unterzeichnen und dem Vertragspartner zustellen kann. X missbraucht Chip-Karte und PIN, indem er damit eine digital signierte Vollmacht erstellt mit der Anweisung an die Bank, dem Arbeitnehmer X das Geld in bar auszuzahlen.

Auf die Rechtslage bezüglich Dissens muss hier nicht näher eingegangen werden, da kein Unterschied besteht, ob die beiden, nicht übereinstimmenden formbedürftigen Willenserklärungen handschriftlich oder mittels digitaler Signatur unterzeichnet wurden. Die herrschende Lehre und Rechtsprechung zum Dissens kann deshalb auch bei Abgabe der Willenserklärungen mittels digitaler Unterschrift angewendet und weitergeführt werden.

Auch elektronisch abgegebene und übermittelte Willenserklärungen können wegen Irrtums (Art. 23ff. OR) angefochten werden.

Beispiel: A vertippt sich beim Schreiben einer Willenserklärung, indem er seine Ware zu FF 100 anstatt zu CHF 100 verkaufen will.

Eine rechtsdogmatische Unterscheidung, ob die Willenserklärung auf konventionellem Weg oder elektronisch erfolgte, ist weder erforderlich noch sinnvoll. Es ist jedoch zu berücksichtigen, dass aufgrund der bereits mehrmals erwähn-

ten Identifikationsmöglichkeit des Absenders, ein Irrtum über die Person des Erklärenden (Art. 24 Abs. 1 Ziff. 2 OR) bei Verwendung der elektronischen Signatur wohl nur noch in seltenen Fällen einen gültigen Anfechtungsgrund darstellt. Es sei denn, der Unterzeichnete habe sich nicht im Verzeichnis der elektronischen Zertifikate eintragen lassen.
Diese Darstellung hat gezeigt, dass im Stadium der Vertragsentstehung keine Gründe ersichtlich sind, die elektronische Signatur in einen besonderen Rechtsrahmen zu stellen. Die allgemeinen Rechtsgrundsätze zur „unterschobenen Erklärung", zum „Dissens" und zur „Irrtumsanfechtung" genügen vollends auch zur rechtsdogmatischen Erfassung der elektronischen Signatur (Dies entspricht auch dem D-Entwurf der ausführt: „Der Entwurf verzichtet auf besondere Regeln über Anfechtung, Zugang und Widerruf elektronischer bzw. elektronisch übermittelter Willenserklärungen. Die allgemeinen Vorschriften des Rechts der Willenserklärung im Bürgerlichen Gesetzbuch, ergänzt durch die von Lehre und Rechtsprechung entwickelten Auslegungskriterien und Wertungen bieten eine hinreichende Grundlage dafür, auch im Bereich des elektronischen Geschäftsverkehrs zu angemessenen und sich in das Gesamtsystem einfügenden Lösungen zu gelangen" [Seite 18]). Im Gegenteil, Sondernormen könnten zu schwierigen Abgrenzungsfragen führen und würden sich damit punkto Rechtssicherheit negativ auswirken. Überdies hätten sie Mühe, gerade die im D-Entwurf so wichtig empfundene Einbettung ins Gesamtrechtssystem zu gewährleisten.
Im Zusammenhang mit den Folgen einer mangelhaften Vertragsentstehung stellt sich u.a. auch die Frage, wem Willenserklärungen zuzurechnen sind, die auf einen missbrauchten privaten Schlüssel zurückgehen bzw. wer den Schaden ersetzen muss, der aus einer solchen Situation entsteht (Siehe Seite 22 des Berichts 2001).
Art. 17 Abs. 3 Satz 2 E-BGES und der Bericht zum Entwurf des E-BGES verweisen im Zusammenhang mit der Haftung auf das Stellvertretungsrecht. Aus den nachfolgenden Überlegungen sind wir jedoch der Meinung, dass stellvertretungsrechtliche Fragen in diesem Zusammenhang keine Rolle spielen und jeglicher Verweis auf das Stellvertretungsrecht deshalb unterbleiben sollte.
Erstens setzt Stellvertretung stets voraus, dass der Vertreter im Namen des Vertretenen handelt (Art. 32 Abs. 1 OR) [Stellvertretung ist Handeln in fremdem Namen (Ausnahme: Art. 32 Abs. 2 OR)], wobei im Zeitpunkt des Vertragsschlusses nur das Vertretungsverhältnis, nicht aber der Name des Vertretenen bekannt sein muss (Bestimmbarkeit genügt); wird das Vertretungsverhältnis im Zeitpunkt des Vertragsabschlusses nicht offengelegt, so kommt der Vertrag nur zustande, sofern es dem Dritten gleichgültig ist, mit wem er den Vertrag abschliesst, was praktisch nur bei Bargeschäften vorkommt (WATTER Rolf, in: Kommentar zum schweizerischen Privatrecht, Obligationenrecht I, Zürich, Bern und Basel 1992, Art. 32 N 20.). Zweitens verlangt Stellvertretung in jedem Fall vom Vertretenen Wissen um das Verhalten des Vertreters. Dies gilt auch für die Anscheins- bzw. Duldungsvollmacht. Stellvertretung liegt nur dann vor, wenn der Vertretene in Kenntnis eines vom Vertreter geschaffenen Anscheins nicht widerspricht (Duldungsvollmacht) oder wenn der Vertretene durch sein Verhalten den Anschein geschaffen hat, dass er dem Vertreter eine Vollmacht bestimmten Inhalts erteilt (BUCHER Eugen, a.a.O., Seite 613). Dazu hält Bucher wörtlich fest: „Die Annahme einer Anscheinsvollmacht ist nur dann gerechtfertigt, wenn das Verhalten des Vertretenen selber als Äusserung eines Bevollmächtigungswillens verstanden werden durfte, nicht jedoch, wenn aufgrund

sonstiger Umstände, infolge eines durch Zufall oder durch Verhalten Dritter entstandenen Rechtsscheins der Dritte auf eine Vertretungsmacht schliessen durfte“. Drittens muss das vom Vertreter vorzunehmende Rechtsgeschäft auch von ihm abgeschlossen werden; wird eine Formvorschrift verlangt, muss der Vertreter seine (eigenhändige bzw. digitale) Unterschrift unter das Dokument setzen.

Aus dem Wortlaut von Art. 16 Abs. 2 und Art. 17 Abs. 1 geht klar hervor, dass der von den Haftungsbestimmungen zu erfassende Sachverhalt von den erwähnten Stellvertretungssachverhalten abweicht. In Art. 16f. geht es darum, die Haftung für den Fall zu regeln, dass der private Schlüssel gegen den Willen des Schlüsselinhabers abhanden gekommen und gebraucht wurde. Dies bedeutet, dass keine der oben erwähnten drei Voraussetzungen erfüllt ist. Das Vertretungsverhältnis wird nicht offengelegt, der Namensgeber weiss nicht um das Verhalten des Dritten und der Dritte setzt nicht seine, sondern die Unterschrift eines Dritten unter das Dokument.

Aufgrund dieser Sach- und Rechtslage sollten Verweise auf das Stellvertretungsrecht im Rahmen der Haftungsnormen des E-BGES unserer Meinung nach unterbleiben. Selbstverständlich sind Stellvertretungshandlungen auch mittels elektronischer Unterschrift möglich. Hier gelten die Normen gemäss Art. 32ff. OR sowie die entsprechende Lehre und Rechtsprechung genau gleich wie bei einer eigenhändigen Unterschrift.

Liegt keine Stellvertretung vor, so kann es sich - wie nachfolgend dargelegt wird - um eine unterschobene Erklärung handeln.

Bei der unterschobenen Erklärung verhält sich ein Dritter derart, dass sein Verhalten als Erklärung eines anderen verstanden wird (und auch nach Treu und Glauben verstanden werden kann).

Wie erwähnt, sind drei mögliche Fälle des Missbrauchs eines privaten Schlüssels (unterschobene Erklärungen) zu unterscheiden, nämlich:

- Die Erklärung erfolgt ohne ursächliche Beziehung zwischen dem Verhalten des vermeintlich Erklärenden und des vermeintlichen Empfängers.
- Das Verhalten des vermeintlich Erklärenden ist ursächlich für den Erklärungsschein beim vermeintlichen Empfänger.
- Das Verhalten des vermeintlich Erklärenden ist ursächlich für den Erklärungsschein beim vermeintlichen Empfänger und zudem trägt Ersterer eine gesteigerte Verantwortung für diese Scheinerklärung.

All diesen Fällen ist gemeinsam, dass die Vertragspartei annimmt, die Erklärung komme von einer anderen Person als dies effektiv der Fall ist. Dass allerdings Stellvertretung ausser Betracht fällt, wurde bereits erwähnt.

Gemäss geltender Rechtslage trägt im ersten Fall der Erklärende keine Verantwortung für die fehlerhafte Willensbildung des Empfängers und ist deshalb auch nicht schadenersatzpflichtig. Im zweiten Fall war der vermeintlich Erklärende Auslöser des Missverständnisses und trägt demnach auch ein Mitverschulden. Im dritten Fall gilt der Vertrag, wie ihn der Empfänger annehmen durfte. Eine Schadenersatzpflicht des vermeintlichen Erklärenden kommt gemäss geltenden Rechtsgrundlagen demnach nur im zweiten Fall in Betracht. Diese Schadenersatzpflicht wollen wir im Folgenden etwas näher betrachten.

Allgemein bestimmt das Haftpflichtrecht, in wie weit ein Schaden vom Geschädigten selber getragen werden muss (*casus sentit dominus*), oder ob der Geschädigte diesen auf einen anderen, meistens den Schädiger, abwälzen kann und welche Voraussetzungen für eine solche Abwälzung vorliegen müssen. Die Haftungstatbestände lassen sich in verschiedene Haftungsarten unterteilen.

Erstens wird zwischen vertraglicher (Eine zivilrechtliche Verantwortlichkeit kann sich aus der Nicht- oder Schlechterfüllung eines Vertrages ergeben [Art. 97ff. OR] oder auch im Zusammenhang mit der Irrtumsanfechtung [Art. 26 OR]) und ausservertraglicher Haftung unterschieden. Im vorliegenden Zusammenhang geht es um die Haftung anlässlich einer fehlerhaften Verwendung einer elektronischen Unterschrift, d.h. die Haftungsfrage stellt sich, bevor überhaupt ein Vertragsverhältnis entsteht. Wir befinden uns deshalb im ausservertraglichen und nicht im vertraglichen Rechtsbereich, d.h. die vertragliche Schlecht- bzw. Nichterfüllung sowie die Irrtumsanfechtung spielen in diesem Zusammenhang keine Rolle. Zweitens unterscheidet die Rechtstheorie zwischen der Verschuldens- und der Kausalhaftung (Zu Einzelfragen siehe OFTINGER Karl/STARK Emil, Schweizerisches Haftpflichtrecht, Allgemeiner Teil, Band I, Zürich 1995, 14 ff. und 44 ff.). Bei der Verschuldenshaftung liegt der Grund einer Schadenersatzpflicht des Schädigers in seinem Verschulden. Die Verantwortung für ein Verhalten setzt jedoch voraus, dass für den Schädiger die Schädigung (Davon wird jedoch bei der Objektivierung der Fahrlässigkeit (teilweise) abgewichen) voraussehbar und deren Folgen für ihn auch erkennbar sind. In der Schweiz gilt die Verschuldenshaftung als allgemeiner Grundhaftungstatbestand, sofern das Gesetz nicht eine Kausalhaftung (einfache Kausalhaftung oder Gefährdungshaftung) vorsieht.
Die Kausalhaftung verzichtet auf die Haftungsvoraussetzung des Verschuldens und damit auch auf die Voraussehbarkeit. Man bezeichnet bestimmte Personen als haftpflichtig, unabhängig davon, ob sie die Möglichkeit der Schädigung durch ihr Tun oder Unterlassen konkret voraussehen konnten. Die Verschuldenshaftung wird mit einem tadelswerten Verhalten, dem Verschulden des Schädigers, gerechtfertigt. Die Kausalhaftung kann demgegenüber auch unabhängig vom Verhalten des Haftpflichtigen, ja sogar unabhängig von einem menschlichen Verhalten (Zufallshaftung), entstehen.
Abschnitt 7 (Art. 16 bis 19) des vorgeschlagenen BGES regelt die Haftung, wobei wir uns im vorliegenden Zusammenhang weder mit der Haftung der Anbieterinnen von Zertifizierungsdiensten (Art. 18) noch mit der Verjährung (Art. 19) noch mit dem Verbot der Aufbewahrung von Kopien privater Signaturschlüssel durch Anbieterinnen von Zertifizierungsdiensten (Art. 16 Abs. 1) auseinandersetzen. Auf die Beweislastverteilung gemäss Art. 17 Abs. 1 werden wir später eingehen.
Kernhaftungstatbestand bildet Art. 17 Abs. 2, der wie folgt lautet: Der Inhaber oder die Inhaberin des privaten Signaturschlüssels haftet der Drittperson für Schäden, die diese deswegen erleidet, weil sie sich auf das gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten verlassen hat.
Gemäss Art. 17 Abs. 3 in Verbindung mit Art. 16 Abs. 2 kann sich der Inhaber eines privaten Signaturschlüssels von seiner Haftung exkulpieren, sofern er den privaten Schlüssel so aufbewahrt, dass eine Verwendung durch unbefugte Drittpersonen ausgeschlossen werden kann und er die hierzu nach den Umständen zumutbaren Vorkehrungen trifft.
Gemäss Bericht (Seite 23) handelt es sich bei dieser Haftung um eine Verschuldenshaftung: wir sind demgegenüber der Ansicht, dass es sich bei der aus Art. 16 Abs. 2 und 17 Abs. 2 und 3 resultierenden Haftung um eine einfache Kausalhaftung handelt.
Im Unterschied zur Verschuldenshaftung (siehe beispielsweise Art. 41 OR) ist bei der Kausalhaftung das Verschulden des Haftpflichtigen nicht Voraussetzung der Haftung. Die Kausalhaftung wird ausgelöst durch eine Sorgfalts-

pflichtverletzung oder einen Mangel und dies auch dann, wenn dadurch wegen ihrer Geringfügigkeit noch kein Verschulden vorliegen würde. Es ist selbstverständlich, dass die Unsorgfalt oft ein Verschulden darstellt; entscheidend für die Abgrenzung zwischen einfacher Kausalhaftung und Verschuldenshaftung ist jedoch, dass die Schuldhaftigkeit nicht zu den vom Gesetz aufgezählten Haftungsvoraussetzungen gehört und folglich vom Geschädigten nicht zu beweisen ist (STARK Emil W., Schweizerisches Haftpflichtrecht, Besonderer Teil I, Band II/1, Zürich 1987, Seite 128). Die einfache Kausalhaftung ist auch von der Verschuldenshaftung mit Beweislastumkehr abzugrenzen, wie sie in der allgemeinen Vertragshaftung zu finden ist (Art. 97 OR) (Die Abgrenzung zwischen Verschuldenshaftung mit umgekehrter Beweislast und einfacher Kausalhaftung war nicht immer klar und wurde im Zusammenhang mit der Tierhalter-, Geschäftsherrenhaftung und der Haftung des Familienoberhaupts erst durch die Rechtsprechung geklärt [zur Haftung des Familienoberhaupts siehe BGE 103 II 124 E. 3]). Im Gegensatz zur Gefährdungshaftung ist der Bestand einer Sorgfaltspflicht genauso Haftungsvoraussetzung wie eine im Gesetz definierte Verletzung dieser Sorgfaltspflicht. Tritt ein Schaden ein, würde bei der Gefährdungshaftung bereits das Verfügen über einen privaten Signaturschlüssel eine Haftung rechtfertigen, demgegenüber braucht es bei der einfachen Kausalhaftung zusätzlich eine Sorgfaltspflichtverletzung (siehe Art. 16 Abs. 2). Als einfache Kausalhaftung gehört deshalb die Haftung gemäss E-BGES zur Familie der Kausalhaftungstatbeständen gemäss dem allgemeinen Haftpflichtrecht. Dazu gehören: Haftung urteilunfähiger Personen (Art. 54 OR), Geschäftsherrenhaftung (Art. 55 OR), Tierhalterhaftung (Art. 56 OR), Werkeigentümerhaftung (Art. 58 OR) und schliesslich auch die Haftung des Familienoberhaupts gemäss (Art. 333 ZGB).

Haftungsgrund ist bei der einfachen Kausalhaftung irgendeine Ordnungswidrigkeit (in concreto: die ungenügend sichere Aufbewahrung des privaten Signaturschlüssels), wobei der Haftpflichtige stets der Inhaber des privaten Schlüssels ist. Im Gegensatz zur Verschuldenshaftung haftet der Kausalhaftpflichtige auch für Fehler anderer, die in seinem Namen gehandelt haben, was eine Haftung analog zur vertraglichen Hilfspersonenhaftung bedeutet (Art. 101 OR).

Die Haftungsregelung gemäss E-BGES würde auch den Haftungsumfang gegenüber der geltenden Rechtslage massgeblich erweitern. Gemäss Art. 17 Abs. 2 haftet der Inhaber eines privaten Signaturschlüssels all jenen gegenüber, die sich auf die gültige digitale Signatur verlassen haben und nun wegen deren Ungültigkeit einen Schaden erleiden. Die Anspruchsberechtigung ergibt sich demnach nicht aus der Person des Geschädigten, dies kann irgendein Dritter sein (Dies beispielsweise entgegen dem stark nachbarrechtlich geprägten Schadenersatznorm gemäss Art. 679 ZGB) und auch nicht aus einer bestimmten physischen (Grundeigentümer- und Tierhalterhaftung) oder rechtlichen (Geschäftsherrenhaftung) Beziehung, sondern alleine aus der Tatsache, dass jemand auf die Gültigkeit einer elektronischen Unterschrift vertraut. Eine auch nur entfernte Beziehung zwischen dem Unterzeichneten und/oder dem Empfänger der elektronischen Signatur ist nicht erforderlich.

Beispiel: A schliesst mit Bauunternehmer B einen Werkvertrag zum Bau einer Garage ab. Die Zahlungsfähigkeit des A entnimmt B aus einer ihm von A überlassenen Kopie einer gefälschten, digital signierten Garantie des Garanten G. Bei Zahlungsunfähigkeit des A würde G dem B für die ausgebliebene Zahlung aus Werkvertrag in der Höhe des Werklohns schadenersatzpflichtig.

Beispiel: Ähnlicher Fall, aber B vertraut auf die Zahlungsfähigkeit des A aufgrund eines gefälschten, mit digitaler Signatur versehenen Schenkungsversprechens des Schenkers S an A.

Der Haftungsumfang der einfachen Kausalhaftung gemäss E-BGES ist damit vom Personenkreis her praktisch nur über den Kausalzusammenhang beschränkt und zwar auch in jenen Fällen, wo zwischen dem Unterzeichneten und dem Geschädigten überhaupt keine Rechtsbeziehung besteht und je bestehen wird. Damit unterscheidet sich die Haftung wesentlich von der heute geltenden Rechtslage im Falle einer aufgrund des Verhaltens des Erklärenden ausgelösten, unterschobenen Erklärung.

Ist der Fall, dass eine unterschobene Erklärung ohne jede Beteiligung des Erklärenden und ohne Verletzung der Sorgfaltspflicht gemäss Art. 16 Abs. 2 zu Stande kommt, beim Gebrauch der digitalen Signatur vermutlich weitgehend ausgeschlossen, so stellt sich die Frage, ob nun bei der Überlassung des privaten Schlüssels in jedem Fall eine Haftung auf negatives Vertragsinteresse entsteht, oder ob der Schlüsselinhaber sich den Vertrag so wie er entstanden ist, entgegenhalten lassen muss. Diese Frage ist deshalb relevant, weil durchaus Konstellationen denkbar sind, wo der Vertragsabschluss im Vergleich zum Vertrauensschaden für den Erklärenden vorteilhafter ist.

Gemäss den allgemeinen Grundsätzen der Beweisführung muss der Geschädigte die Haftungsgrundlagen (Schaden, Kausalzusammenhang, Widerrechtlichkeit, resp. Vertragsverletzung bei der Vertragshaftung) beweisen. Ihm werden in gewissen Fällen jedoch Erleichterungen gewährt; so muss zum Beispiel der Kausalhaftpflichtige dartun, dass er alles zur Vermeidung des Schadens vorgekehrt hat (siehe Art. 16 Abs. 2), und bei der Haftung aus Vertrag wird das Verschulden vermutet. Kann dieser Entlastungsbeweis nicht geführt werden, so haftet der Inhaber des privaten Schlüssels für sämtliche Schäden, die Dritte erleiden, weil sie auf die Gültigkeit des Schlüssels vertraut haben.

Gemäss Art. 8 ZGB hat grundsätzlich derjenige das Vorhandensein einer behaupteten Tatsache zu beweisen, der aus ihr Rechte ableitet. Dies bedeutet, dass jede Partei die tatbeständlichen Voraussetzungen desjenigen Rechtssatzes zu beweisen hat, der zu ihren Gunsten wirkt (Kummer Max, Berner Kommentar zum Schweizerischen Zivilgesetzbuch, Band I/1, Bern 1962, N 132 zu Art. 8).

Von diesem allgemeinen Rechtsgrundsatz kann das Gesetz Ausnahmen vorsehen (so Art. 8 ZGB ausdrücklich). Art. 17 Abs. 1 regelt die Beweisführung und bestimmt, dass der Inhaber eines privaten Signaturschlüssels beweisen muss, dass dieser ohne seinen Willen eingesetzt wurde. Diese Beweislastumkehr ist aus unserer Sicht sowohl materiell als auch bezüglich ihrer systematischen Einordnung problematisch.

Systematisch gehört unseres Erachtens Art. 17 Abs. 1 E-BGES nicht in den Abschnitt 7 (Haftung), sondern ordnet die fehlerhafte Entstehung der Willenserklärung. Die Ursache dieser fehlerhaften Willensbildung ist offen und kann sowohl auf einer unterschobenen Erklärung, einem Dissens oder einem Irrtum basieren.

Materiell würde Art. 17 Abs. 1 bedeuten: Misslingt der Beweis, ist der Vertrag rechtsgültig zustandegekommen (siehe Bericht Seite 22). Diese Rechtsfolge würde eine grundsätzliche Änderung der geltenden Theorien im Zusammenhang mit „unterschobener Erklärung“, „Dissens“ und „Irrtum“ bedeuten.

Beispiel: A und B führen Vertragsverhandlungen. Gemäss den allgemeinen Vertragsbestimmungen tritt der Vertrag in Kraft, sobald er von beiden Parteien

unterzeichnet ist. Der erste von B ausgefertigte Vertragsentwurf liegt vor und wird A mittels E-Mail von B zugestellt. A speichert diesen in einem File ab und liest ihn oberflächlich am Bildschirm. Dabei realisiert er, dass der Vertrag in Hauptpunkten von seinen Vorstellungen abweicht. Über Nacht wird der Vertragsentwurf - gegen den Willen des A - digital signiert und B elektronisch zugestellt.

Misslingt A der Entlastungsbeweis, dass nicht er, sondern ein anderer den Vertrag digital unterzeichnet hat, so gilt der Vertrag, wie wenn der Inhaber den Vertrag selber abgeschlossen. Dies würde nicht nur den geltenden Regeln über den Dissens widersprechen, sondern einen Teil unserer heutigen Rechtsordnung verändern. Gründe, weshalb für digital unterzeichnete Dokumente eine völlig neue Rechtslage entstehen soll, sind nicht ersichtlich. Geht man davon aus, dass die Beweislast dem Schlüsselinhaber eher zugemutet werden kann als dem Empfänger der Willenserklärung, so muss diese Beweislastumkehr generell, und nicht im BGES, geregelt werden (siehe dazu Art. 56d Abs. 2 des Entwurfs für eine Revision und Vereinheitlichung des Haftpflichtrechts).

Gründe für eine Regelung der Beweislastumkehr wie sie Art. 17 Abs. 1 vorsieht, sind nicht ersichtlich. Auch ohne diese Beweislastumkehr gilt heute der Grundsatz von Treu und Glauben auch im Zusammenhang mit der Beweislast. Behauptet der Kläger, nachdem er von der elektronischen Unterschrift Kenntnis erhalten hat, der Vertrag sei zu Stande gekommen, so muss der Beklagte, der geltend machen will, der private Signaturschlüssel sei ohne seinen Willen verwendet worden, dies wirksam bestreiten. Der Kläger kann sich anschliessend im Rahmen des Beweises auf diese wirksam bestrittenen Faktoren beschränken. Damit findet auch dann eine Art Beweislastumkehr statt, wenn das materielle Recht eine solche nicht explizit festlegt (Siehe dazu BRÖNIMANN Jürgen C., Die Behauptungs- und Substanzierungslast im schweizerischen Zivilprozessrecht, Bern 1989, Seiten 221ff.).

Schliesslich führt Art. 17 Abs. 1 zu neuen Abgrenzungsschwierigkeiten. Gelingt der Beweis nicht, so muss sich der Schlüsselinhaber den Vertrag in seiner vollen Form entgegenhalten lassen (Bericht 2001, Seite 22). Der Vertrag entfaltet volle Gültigkeit und Rechtsbeständigkeit. Kann der Beweis nicht geführt werden und hat der Inhaber des privaten Schlüssels auch die Sorgfaltspflicht gemäss Art. 16 Abs. 2 nicht erfüllt, so stehen sich zwei unterschiedliche Rechtsfolgen gegenüber (Vertrag kommt nicht zu Stande, ausservertraglicher Schadenersatz einerseits, Vertrag kommt zustande, andererseits), die sich gegenseitig ausschliessen; eine Klärung ist deshalb dringend erforderlich.

Die Haftungsnormen verschärften die Haftung des Inhabers eines privaten Signaturschlüssels in dreifacher Hinsicht:

1. Aus der üblichen Verschuldenshaftung wird gemäss E-BGES eine einfache Kausalhaftung
2. Der Haftungsumfang wird gegenüber anderen, ähnlichen Kausalhaftungsnormen, in Bezug auf den Schadenersatzberechtigten faktisch wesentlich ausgeweitet
3. Die Beweislastumkehr auferlegt dem Schlüsselinhaber ein zusätzliches Risiko im Falle der Beweislosigkeit.

Aufgrund dieser Erwägungen sind wir der Meinung, dass im E-BGES auf haftungsrechtliche Sondernormen verzichtet werden sollte. Eine unverhältnismässig strenge Haftung kann die angestrebte breite Akzeptanz für das neue Rechtsinstitut der elektronischen Signatur gefährden.

Aus sich selbst heraus handelt es sich bei der Kernnorm (Art. 17 Abs. 2) um eine Gefährdungshaftung, da die Norm selber keine Verletzung einer vorausgesetzten Sorgfaltspflicht verlangt. Eine Kausalhaftung setzt demgegenüber das Bestehen einer Sorgfaltspflicht voraus, deren Verletzung dem Betroffenen zum Vorwurf gemacht wird. Eine solche Sorgfaltspflicht auferlegt Art. 16 Abs. 2, der besagt: Die Inhaber und Inhaberinnen privater Signaturschlüssel müssen diese so aufbewahren, dass eine Verwendung durch unbefugte Drittpersonen ausgeschlossen werden kann. Sie treffen hierzu nach den Umständen zumutbaren Vorkehrungen.

Die Beziehung zwischen den beiden Rechtsnormen wird schliesslich durch Art. 17 Abs. 3 hergestellt. Erst das Zusammenwirken dieser drei Normen gibt dem Haftungstatbestand seinen definitiven Inhalt und definiert ihn als einfache Kausalhaftung. Im Interesse der Klarheit sind wir deshalb der Ansicht, dass die Haftung in einer Norm zusammengefasst werden sollte.

Eine wichtige Frage im Zusammenhang eines Kausalhaftungstatbestandes ist die Definition der vorausgesetzten Sorgfalt. Das E-BGES fordert „alle nach den Umständen zumutbaren Vorkehrungen“, womit es von den Haftungsnormen gemäss den Art. 54ff. OR, die von einer „gebotenen Sorgfalt“ sprechen, abweicht. Es stellt sich hier deshalb die Frage, ob mit dieser Abweichung eine materielle Differenzierung beabsichtigt ist.

KVN In diesem Artikel sollte klar verankert werden, dass jegliche anders lautende vertragliche Abmachungen nichtig sind.

Muster/Sury Bei der Haftung wird nicht geregelt, für welche Schäden die Anerkennungsstelle aufkommen muss, wenn sie ihren Pflichten der sorgfältigen Auswahl einer Zertifizierungsstelle nicht erfüllt und ob eine Regressmöglichkeit von Seiten der Geschädigten besteht.

Rosenthal Auf die Problematik des Bedeutungsgehalts einer Signatur wurde in Punkt 3.1 bereits hingewiesen, ebenso darauf, dass Art. 17 Abs. 1 nicht viel mit „Haftung“ zu tun hat. Gemäss den Ausführungen der Verfasser des BGES-VE (Erläuterungen, Nr. 210.072) muss angenommen werden, dass es sich bei Abs. 1 um eine Spezialnorm zur Beweislastregelung im Rahmen des Stellvertretungsrechts *des OR* und nicht um eine generelle, für alle Rechtsbereiche geltende Norm handeln soll. Eine diesbezügliche Einschränkung wäre darum empfehlenswert, soll Art. 17 Abs. 1 an der bisherigen Stelle verbleiben.

Die in Art. 17 Abs. 1 getroffene Regelung – wird sie im Sinne der Verfasser des BGES-VE interpretiert – wird dafür sorgen, dass Dritte einer signierten Willenserklärung a priori nicht trauen dürfen. Daran ändert auch die Haftungsnorm des Art. 17 Abs. 2 nichts, wenigstens wenn demjenigen, der einer Signatur dennoch vertraut hat (Was nach dem Gesagten streng genommen sogar zu einem Mitverschulden des Geschädigten führen könnte), gemäss Erläuterungen nur das negative Vertragsinteresse ersetzt werden soll.

Art. 17 bietet somit keine genügende Rechtssicherheit für die Empfänger von Signaturen. Wird der Bedeutungsgehalt einer Signatur so verstanden, wie ihn die Verfasser des BGES-VE verstehen, so muss der Empfänger einer signierten Erklärung jederzeit damit rechnen, dass ihm der Inhaber einer Signatur eröffnet, dass er die signierte Erklärung nicht erzeugt und nicht gewollt habe und er darum auch nicht daran gebunden sei (ob und wie häufig dies in der Praxis vorkommen wird, ist eine andere Frage, auch wenn davon ausgegangen werden muss, dass die hier geführten Diskussionen sich um eher seltene Tatbestände drehen).

Die Verfasser des BGES-VE begründen diese Regelung mit dem Verweis auf die allgemeinen Regeln des Stellvertretungsrechts im Falle des vollmachtlosen Vertreters. Sie übersehen dabei, dass zwischen dem typischen Fall des Geschäfts eines vollmachtlosen Stellvertreters und der Benutzung einer Signatur durch eine unbefugte Person ein Unterschied besteht: Der Geschäftspartner eines vollmachtlosen Stellvertreters, der sich einer Signatur bedient, kann gar nicht erkennen können, dass hier ein Fall der Stellvertretung vorliegt (oder nicht). Der Dritte sieht der Signatur nicht an, von wem sie erzeugt wurde. Dennoch soll er dem Risiko eines nicht zustande gekommenen Vertrags ausgesetzt werden, sollte der Vertretene den Vertrag nicht genehmigen und seine fehlende (interne) Vollmacht beweisen. Hier zeigt sich der Systemunterschied zur eigenhändigen Unterschrift, die immer vom Unterzeichner persönlich geleistet werden muss, und einer Signatur, die biologisch nicht mit ihrem rechtlichen Inhaber verknüpft ist.

Natürlich ist es nicht ungewöhnlich, dass sich eine Geschäftsperson nicht dafür interessiert, ob ihr Gegenüber in einem Geschäft der Vertragspartner höchstpersönlich oder nur dessen Vertreter ist. Es steht ihr jedoch frei, diese Abklärung zu treffen, falls sie das will. Daran ändert der Einwand nichts, dass ein Betrüger sich auch im Geschäftsleben „ausserhalb“ des Internets für eine andere Person ausgeben kann. In solchen Fällen liegt kein Stellvertretungsverhältnis vor, da der Betrüger nicht im Namen eines anderen, sondern unter dem Namen eines anderen handelt. Kommt es zu einem solchen Fall – ob mit Signaturen und entsprechenden Erklärungen im elektronischen Geschäftsverkehr oder mit einem gestohlenen Ausweis im traditionellen Geschäftsverkehr –, so wird die Person, für die sich der Betrüger ausgibt, nicht verpflichtet.

Im elektronischen Geschäftsverkehr mit Signaturen wird der Betrüger aber typischerweise nicht so weit gehen müssen, da im Rahmen einer Signatur aus der Sicht des Empfängers nicht zwischen einer Erklärung durch den Vertragspartner selbst und einer Erklärung durch einen Vertreter unterschieden wird. Es wird immer der Name nur des Vertretenen erscheinen; das bei eigenhändigen Unterschriften durch einen Vertreter übliche „i.A.“ ist in einer Signatur implizit mitenthalten.

Letztlich muss davon ausgegangen werden, dass eine Person sich ein gesetzlich anerkanntes Zertifikat nur dann ausstellen lassen wird, wenn sie damit rechtsverbindliche Erklärungen abgeben können will, ohne dass eine weitere Betätigung ihrerseits nötig ist. Sie wählt das Instrument der Signatur gerade wegen und nicht trotz seiner Funktionsweise, wovon sie zwar profitiert, aber eben auch Risiken eingeht. Das Missbrauchsrisiko ist der Preis der Effizienz. Das ist auch in vielen anderen Bereichen des alltäglichen Geschäftsverkehrs so (Wobei wiederum auf das Beispiel der Geldautomatenkarte verwiesen werden kann). Wesentlich ist, dass sie über diese Konsequenzen informiert wird, was nach Art. 10 Abs. 2 vorgesehen ist.

Die bestehende Regelung im BGES-VE wird dieser Sachlage nicht gerecht. Sie privilegiert den Inhaber einer Signatur stark, womit letztlich auch der Wert einer Signatur im Geschäftsverkehr massiv reduziert wird. Damit wird auch dem Inhaber einer Signatur nicht gedient sein. Er hat zwar ein geringeres Haftungsrisiko, doch ein gewisses, mitunter abschreckendes Risiko bleibt. Umgekehrt ist die Signatur für potentielle Empfänger möglicherweise nicht soviel wert, dass sie Benutzer solcher Signaturen im Geschäftsverkehr privilegieren werden.

Nach Ansicht des Verfassers dieser Stellungnahme sollte der gute Glaube des Signatur-Empfängers wenigstens teilweise geschützt werden. Die bestehende

Lösung des Art. 17 Abs. 1 stellt lediglich auf den Willen des Vertretenen ab, der als rein interner „Faktor“ des Signatur-Inhabers der Wahrnehmung des Empfängers der Signatur vollständig entzogen ist. Der Empfänger hat typischerweise keine Möglichkeit, den wahren Willen des Vertretenen zu ermitteln (Er muss diesen bei Vertragserklärungen auch nicht ermitteln, da diese im Schweizer Vertragsrecht im Streitfall nach dem Vertrauens- und nicht dem Willensprinzip ausgelegt werden müssen), doch genau darauf soll es ankommen.
Der in Art. 17 Abs. 1 vorgesehene Beweis dürfte darum in vielen Missbrauchsfällen nicht sehr schwer zu erbringen sein, sofern der Inhaber der Signatur den Richter mit Zeugen aus seinem Umfeld überzeugen kann, dass die abgegebene und signierte Erklärung für ihn unsinnig ist, wie etwa der Kauf eines Gegenstands zur Lieferung an eine ihm fremde Person. Da es gemäss den Erläuterungen und Art. 17 Abs. 1 nur auf den (wahren) Willen des Vertretenen ankommen soll, spielt es keine Rolle, ob der Dritte hätte erkennen können, dass die Erklärung für den Vertretenen unsinnig ist.
Eine bessere Lösung wäre darum, den gesetzlichen (aber umstrittenen) Gutglaubensschutz von Art. 33 Abs. 3 OR (oder ggf. Art. 34 Abs. 3 OR, je nach Betrachtungsweise) analog oder direkt zur Anwendung zu bringen. Dies hätte zur Folge, dass der Inhaber einer Signatur für deren Einsatz zunächst solange einstehen müsste, als der Dritte gutgläubig ist. Dieser gute Glaube kann zum Beispiel durch einen sicherheitsbedingten Rückzug des Zertifikats zerstört werden. Allerdings ist ein Zertifikat dabei nicht mit einer Vollmacht im herkömmlichen Sinne zu vergleichen, die ebenfalls zurückgezogen werden kann, sollte sie nicht mehr bestehen. Das Zertifikat ist vielmehr die Kundgabe einer Bevollmächtigung an Dritte, die die Basis des Gutglaubensschutzes darstellt.
Im Falle gesetzlich anerkannter Signaturen von natürlichen Personen muss eingeräumt werden, dass der Einsatz einer Signatur durch eine andere als die aufgeführte Person in den meisten Fällen missbräuchlich sein wird. Mit einem Gutglaubensschutz würde auch die Haftungsregelung des Abs. 2 und 3 deutlich an Gewicht verlieren. Der gutgläubige Dritte wird der Signatur und der damit zumindest auf die dem Anschein nach damit verbundenen Erklärung eines Rechtsbindungswillens der angeführten Person vertrauen. Sein Schutz wird jedoch aufgrund des heutigen Stellvertretungsrechts nur soweit gehen, als es der Signaturinhaber in der Hand hat, den Einsatz seines Signaturschlüssels bzw. seines Zertifikats zu kontrollieren. Erst wenn der in Art. 17 Abs. 3 vorgesehene Ausnahmefall einer Kompromittierung des privaten Schlüssels trotz sorgfältigem Verhalten des Signaturinhabers eintritt, erscheint es angebracht, den Vertrauensschutz des Dritten aufzuheben oder einzuschränken, sofern dieser dann überhaupt noch gutgläubig sein kann.
Es wird darum empfohlen, hinsichtlich der Rechtswirkung von Signaturen im Vertragsrecht ausdrücklich eine Regelung vorzusehen, die den gutgläubigen Dritten schützt. Das Institut der Anscheinsvollmacht kann hier eine gute Vorlage liefern. Auch bei einer solchen muss der Vertretene nicht in jedem Falle haften. So wird für die Annahme einer Anscheinsvollmacht verlangt, dass der Vertretene das Verhalten des Vertreters bei pflichtgemässer Aufmerksamkeit kennen und verhindern könnte (BGE 120 II 201). Konnte er dies nicht, kommt der Gutglaubensschutz nicht zum Zuge und der Vertretene wird nicht gebunden. Das lässt sich analog oder direkt auch auf Signaturen anwenden. Dies würde für die nötige Sicherheit im Verkehr sorgen.

Am Rande sei bemerkt, dass die Regelung von Art. 17 Abs. 1 begrifflich so ausgestaltet ist, dass ein Rechtsanwender sie auf jede Signatur anwenden könnte, nicht nur auf solche, die mit einem anerkannten Zertifikat verbunden sind. Es wäre darum empfehlenswert, wenn Abs. 1 diesbezüglich präzisiert würde. Dies gilt auch für Art. 16 Abs. 2.

Eine Schadenersatzpflicht für Inhaber von Signaturen, die mit ihrem privaten Signaturschlüssel nicht sorgfältig umgehen, ist nach Ansicht des Verfassers dieser Stellungnahme sinnvoll, soweit sich eine Bindungswirkung der signierten Erklärungen nicht schon aus dem Stellvertretungsrecht ergibt.

Die bestehende Regelung hat jedoch gewisse Mängel. Zunächst wird aus Art. 16 Abs. 2 nicht klar, welche Schutzmassnahmen verlangt werden können. Damit ist nicht ein Ruf nach technischen Einzelheiten verbunden; solche sollten nicht im BGES geregelt werden. Unklar ist jedoch, ob die verlangten Schutzmassnahmen für die betreffende Person nur subjektiv oder aber objektiv zumutbar sein müssen. Zudem stellt sich die Frage, auf welche Umstände abgestellt wird. Es kann nach Ansicht des Verfassers dieser Stellungnahme nicht sein, dass für unterschiedliche Personenkreise unterschiedliche Sicherheitsstandards gelten. Genau diese Gefahr droht jedoch bei der gegenwärtigen offenen Formulierung des Art. 16 Abs. 2.

Ein zweiter Mangel ist die fehlende Regelung der Beweislast in Art. 17 Abs. 3. Der Verfasser der Stellungnahme geht davon aus, dass der Geschädigte beweisen muss, dass der Inhaber der Signatur seinen Schutzverpflichtungen nicht nachgekommen ist. Dies wird realistischerweise nur schwer möglich sein, auch wenn die Praxis in solchen Fällen eine gewisse Mitwirkungspflicht des Signatur-Inhabers annehmen wird. Es stellt sich jedoch die Frage, ob nicht auch hier eine explizite Beweislastregelung am Platz wäre. Sie könnte den vorprogrammierten Streit um die Beweislastverteilung von Art. 17 Abs. 2 und 3 verhindern. Denn es lässt sich mit guten Argumenten vertreten, dass schon die jetzige Fassung des Art. 17 Abs. 3 vorsieht, dass der Signatur-Inhaber und nicht der Geschädigte beweisen muss, dass er alle nötigen Schutzmassnahmen eingehalten hat.

Ein weiteres Manko ist schliesslich die Frage, wofür Schadenersatz geleistet werden muss. Art. 17 Abs. 2 und 3 kann nicht nur für Fälle der vollmachtlosen Stellvertretung angerufen werden, sondern nach dem Wortlaut von Abs. 2 in allen Fällen, in denen eine Person einem Zertifikat „vertraut“ hat (ein Beispiel ist etwa der Einsatz in Kombination mit einer herkömmlichen Kreditkartennummer, die sich danach als gestohlen herausstellt). Diese Formulierung ist sehr breit und sehr vage. Es ist zudem nicht ersichtlich, warum Abs. 2 nur den Ersatz des negativen Vertragsinteresses gewährt, wie das die Verfasser des BGES-VE annehmen.

Vgl. auch zu Art. 3 und 18 / Cf. également ad art. 3 et 18 / Cfr. anche ad art. 3 e 18.

SAV Pour que les utilisateurs comprennent bien les risques qu’ils encourent en relation avec l’utilisation de certificats, il serait préférable de se référer à des situations existant déjà, plutôt que de créer de nouvelles normes de responsabilité. Il suffirait ainsi de préciser que le titulaire du certificat répond d’une utilisation abusive de sa signature électronique comme il répondrait de l’utilisation abusive de blanc-seing, l’effet juridique de documents ainsi signés étant en principe identique à celui de documents produits à partir de blanc-seings, à l’insu du signataire. Cela n’exclut pas a priori l’application également des règles sur la représentation sans pouvoir comme proposé dans le projet de loi.

Un cas différent de l'utilisation abusive est celui de l'utilisation de la signature électronique par un représentant, avec le consentement du titulaire, par exemple parce que le représentant n'a pas encore de signature propre et que le titulaire ne peut momentanément signer lui-même. Vu l'absence de signature sociale et l'exclusion des pseudonymes, un document produit de cette façon pourrait être considéré comme un faux au sens du droit pénal. Il serait aussi possible de considérer qu'il s'agit d'un cas de représentation légitime, mais dans ce cas il faudrait modifier les dispositions sur la représentation.

Die Bestimmungen des Obligationenrechts über die Stellvertretung (Art. 32 ff. OR) sollten mit einer Bestimmung ergänzt werden, wonach das befugte Handeln unter fremdem Namen, insbesondere das befugte Verwenden fremder Legitimationsmittel unter Abwesenden, die gleichen Rechtswirkungen hat, wie das Handeln im fremden Namen im Sinne von Art. 32 Abs. 1 OR.

Schlauri/Kohlas Die wohl naheliegendste Möglichkeit, eine digitale Signatur zu fälschen, besteht darin, den Signierschlüssel durch Einbruchsversuche oder Virenattacken gegen den Computer, auf dem sich das Signiersystem befindet, zu entwenden. Die Fälschungsprävention wird dadurch erschwert, dass herkömmliche Computersysteme zu komplex sind, als dass ein normaler Anwender die zum Betrieb eines nicht speziell gesicherten Signiersystems nötige hohe Sicherheit selbst schaffen könnte.

Der Signierschlüsselinhaber hat a priori gar kein Interesse am Einsatz eines sicheren Systems, weil ein unsicheres System den Echtheitsnachweis seines Prozessgegners leichter ins Wanken bringen kann als ein gut gesichertes. Um digitale Signaturen im Rechtsverkehr verlässlich zu machen, muss das Interesse an einem sicheren System auf dem Wege der Gesetzgebung geschaffen werden, indem für Missbrauchsfälle eine Haftung des Signierschlüsselinhabers statuiert wird. Art. 17 Abs. 2 bestimmt denn auch, dass der Signierschlüsselinhaber gegenüber Drittpersonen grundsätzlich für Schäden haften soll, die diese erleiden, weil sie sich auf ein gültiges Zertifikat verlassen haben. Auf der anderen Seite lassen sich Restrisiken natürlich nicht ganz ausschliessen, und es wäre unbillig, den Signierschlüsselinhaber auch dann haften zu lassen, wenn er alle zumutbaren Massnahmen zur Absicherung getroffen hat. Dem tragen die Art. 17 Abs. 3 und 16 Abs. 2 Rechnung, indem sie die Haftung für diesen Fall ausschliessen. Diese Regelung ist in dieser Form grundsätzlich zu begrüssen.

In diesem Zusammenhang stellt sich die Frage, was unter zumutbaren Massnahmen zur Absicherung zu verstehen sein soll. Dabei sind insbesondere die beschränkten Fachkenntnisse des Signierschlüsselinhabers zu berücksichtigen.

Der Vorentwurf sieht in Art. 10 Abs. 2 Satz 2 für die Zertifizierungsdiensteanbieter eine Informationspflicht über geeignete Massnahmen zur Geheimhaltung des Signierschlüssels vor. Dazu gehört selbstverständlich auch die Information über die Auswahl eines geeigneten Signiersystems, weil dieses für die Sicherheit des Signierschlüssels elementar ist. Dabei ist u.E. auch darauf hinzuweisen, welche zusätzlichen Sicherheitsmechanismen nebst dem Einsatz eines Systems für einen sicheren Betrieb nötig sind, und dem Computerlaien ist vom Betrieb von Systemen abzuraten, die ihn diesbezüglich überfordern. Weil der Schlüsselinhaber in der Regel nicht selbst beurteilen kann, welche Sicherheitsvorkehrungen nötig sind, dürften die Empfehlungen des Zertifizierungsdiensteanbieters gleichzeitig auch die Grenze dessen darstellen, was von ihm

an Sicherheitsmassnahmen verlangt werden, bzw. was als zumutbar im Sinne von Art. 16 Abs. 2 gelten kann.
Nach Art. 18 Abs. 1 haften die Zertifizierungsdiensteanbieter sowohl gegenüber den Signierschlüsselinhabern als auch gegenüber Drittpersonen für Schäden, die sich aus einer Verletzung ihrer Pflichten aus dem BGES ergeben. Falls sich ein Signierschlüsselinhaber gestützt auf Art. 17 Abs. 3 aufgrund ungenügender Information durch den Zertifizierungsdiensteanbieter bei einem Missbrauch seines Signierschlüssels exkulpieren kann, muss u.E. der Zertifizierungsdiensteanbieter dem Dritten für den entstandenen Schaden haften.
Die Informationspflichten gemäss Art. 10 Abs. 2 entsprechen wortwörtlich denjenigen von Art. 9 Abs. 2 der ZertDV und sind damit bereits geltendes Recht. Sie werden allerdings auch im vorliegenden Entwurf der Ausführungsbestimmungen zur ZertDV vom 9. Januar 2001 nicht weiter konkretisiert. Einerseits in Anbetracht möglicher Interessenkonflikte der Zertifizierungsdiensteanbieter und andererseits aufgrund der offenen Formulierung auch des neuen Art. 10 Abs. 2 VE-BGES und des sich daraus für die Zertifizierungsdiensteanbieter ergebenden Subsumtionsrisikos ist u.E. darauf zu drängen, die Informationspflicht bezüglich Auswahl sicherer Signiersysteme und sicherer Konfiguration des Computersystems in den Ausführungsbestimmungen weiter zu konkretisieren.
Der direkte Nachweis für den Missbrauch eines Signierschlüssels auf dem Wege technischer Untersuchungen wird nur sehr selten zu erbringen sein, weil es mangels Spuren in der Regel ausserordentlich schwierig ist, auf einem Computersystem frühere Abläufe wie Hacker- oder Virenangriffe zu rekonstruieren. Andererseits ist aber auch der Nachweis des Gegenteils ausgesprochen komplex und weist eine Reihe von Unwägbarkeiten auf: Alle zur Erstellung der Signatur notwendigen Schritte müssen im Sinne einer Indizienkette bewiesen werden, was dem Prozessgegner des Signierschlüsselinhabers wohl nur selten gelingen kann.
Der Vorentwurf macht den Signierschlüsselinhaber für den Missbrauch des Signierschlüssels beweispflichtig (Art. 17 Abs. 1), kehrt also die Regelung des Art. 8 ZGB um. Dieses Vorgehen greift u.U. weit in materielle Rechtspositionen des Signierschlüsselinhabers ein (Haftung für das positive Vertragsinteresse!), weshalb sie nur aus gutem Grund erfolgen sollte.
Die Beweislastumkehr zugunsten des auf die Signatur vertrauenden Dritten ist u.E. aufgrund von Billigkeitsüberlegungen gerechtfertigt: Denn es liegt im ausschliesslichen Einflussbereich des Signierschlüsselinhabers, das Risiko einer Schlüsselkompromittierung durch den Einsatz eines sicheren Signiersystems und durch Geheimhaltung der entsprechenden Zugangsdaten zu minimieren. Auch hat der Signierschlüsselinhaber in einem Prozess trotz der sich auch ihm stellenden technischen Schwierigkeiten wohl eine tendenziell bessere Ausgangslage: Er könnte beispielsweise unter Umständen durch Zeugen indirekt beweisen, dass es ihm zum fraglichen Zeitpunkt gar nicht möglich war, eine digitale Signatur zu erstellen. Ferner wird der Signierschlüsselinhaber über die Risiken aufgeklärt, bedient sich der digitalen Signatur grundsätzlich freiwillig und hat erst noch die Möglichkeit, seine Haftung im Zertifikat summenmässig zu beschränken (wenngleich ihm letzteres im Falle einer Serie von Missbräuchen u.U. nur wenig hilft).
Fragen kann man sich, ob die Beweislastumkehr tatsächlich in einer derartigen Absolutheit erfolgen soll: In der Bundesrepublik Deutschland liegt derzeit der Referentenentwurf vom 6. September 2000 für ein „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen

Rechtsgeschäftsverkehr“ vor, gemäss dem eine in elektronischer Form vorliegende Willenserklärung nach Prüfung aufgrund des Signaturgesetzes als echt gilt, solange nicht Tatsachen es ernsthaft als möglich erscheinen lassen, dass sie nicht mit dem Willen des Signierschlüsselinhabers abgegeben wurde (so der Vorschlag für einen neuen § 292a ZPO). Anders als der schweizerische Vorentwurf, der eine Vermutung für den korrekten Einsatz des Signierschlüssels vorsieht und damit den Beweis des Gegenteils verlangt, statuiert eine solche Formulierung bloss einen Anschein für den korrekten Einsatz, der schon durch die blosse ernsthafte Möglichkeit eines anderen Verlaufs wieder umgestossen werden kann.

Eine vollständige Beweislastumkehr im Sinne des Schweizer Vorentwurfs führt beispielsweise dazu, dass auch der Nachweis des Befalls des Signiersystems durch einen Virus, welcher bekanntermassen Signaturen fälscht, nicht ausreicht, um den Echtheitsbeweis zu erschüttern. Notwendig ist auch diesfalls weiterhin der (wohl regelmässig indirekte) Nachweis, dass der Signierschlüsselinhaber die Signatur tatsächlich nicht gesetzt hat. Der deutsche Vorschlag hingegen würde eines solchen Nachweises wohl nicht mehr bedürfen und verschöbe die Beweislast wieder auf die Gegenpartei.

Die Problematik des deutschen Vorschlags besteht jedoch darin, dass es oftmals allein in der Macht des Signierschlüsselinhabers läge, einer ihm nicht genehmen Signatur nachträglich durch Manipulationen am eigenen System die erhöhte Beweiskraft wieder zu rauben. Er könnte beispielsweise sein System nachträglich gezielt mit einem Virus verseuchen, worauf es tatsächlich als „ernsthaft möglich“ erscheint, dass die Willenserklärung nicht mit dem Willen des Signierschlüsselinhabers gesetzt wurde. Auf dem Wege der Rechtsprechung – durch Auslegung des unbestimmten Rechtsbegriffs der ernsthaften Möglichkeit – könnten derartige Auswüchse zwar korrigiert werden (etwa indem für einen Nachweis der Möglichkeit einer Fälschung durch einen Virus der Virenbefall zum angeblichen Zeitpunkt des Signierens nachgewiesen werden muss), dies führte allerdings wohl wieder zu einem ähnlichen Ergebnis wie die bedeutend elegantere Beweislastumkehr des Art. 17 Abs. 1 VE-BGES.

Aus diesen Gründen ist die Beweislastumkehr des Art. 17 Abs. 1 u.E. gerechtfertigt.

Das Verbot der Aufbewahrung von Signierschlüsselkopien ist in Art. 16 Abs. 1 im 7. Abschnitt (Haftung) systematisch falsch platziert. Korrekt wäre die Regelung im 3. Abschnitt (Generierung und Verwendung der kryptographischen Schlüssel), denn die Aufbewahrung von Kopien der Schlüssel steht in engem Zusammenhang mit deren Generierung und hat mit der Haftung nichts zu tun.

Die Überschrift des 3. Abschnittes wäre überdies anzupassen.

Weil private Schlüssel in falsche Hände geraten (kompromittiert werden) können, braucht es einen Mechanismus, um Zertifikate für ungültig deklarieren oder Signierschlüssel zurückziehen (revozieren) zu können. Ohne auf eine konkrete Zeitstempelinfrastruktur einzugehen, zeigen wir einige Probleme, die sich beim Aufbau einer solchen Infrastruktur ergeben. Insbesondere soll gezeigt werden, dass im Zusammenhang mit der Zertifikatsrevokation die Rolle von Zeitstempeldiensten gesetzlich zu regeln ist.

Zunächst muss eine Präzisierung der in der Praxis oft schwammig verwendeten Begriffe der Schlüssel- resp. Zertifikatsrevokation erfolgen. Eine mögliche Interpretation von Schlüsselrevokation ist, dass ein Schlüsselinhaber nicht mehr länger einen bestimmten Signaturschlüssel verwenden will, und deshalb alle für seinen Schlüssel und seine Person ausgestellten Zertifikate ungültig werden

sollen. Unter Zertifikatsrevokation wäre dann der Spezialfall zu verstehen, dass nur ein bestimmtes Zertifikat nicht mehr gültig sein soll, zum Beispiel ein bestimmtes Attributzertifikat.
Es stellt sich sodann die Frage, wann ein Zertifikat als revoziert gelten soll: Der auf das Zertifikat vertrauende Dritte muss die Möglichkeit haben, von der Revokation Kenntnis zu nehmen. Aus Gründen der Rechtssicherheit muss der Zeitpunkt, zu dem ein Zertifikat als revoziert gelten soll, mit der erstmaligen Möglichkeit zur Kenntnisnahme übereinstimmen. Eine Möglichkeit zur Sicherstellung dieser Kenntnisnahme besteht darin, dass der Zertifizierungsdiensteanbieter periodisch und in kleinen Abständen eine Liste der Zertifikate (die Certificate Revocation List) veröffentlicht, die nicht mehr gültig sind.
Dies wird im Vorentwurf denn auch so geregelt, was zu begrüssen ist.
Rückdatierungsproblem. Einer in einem digital unterschriebenen Dokument enthaltenen Zeitangabe kann nicht vertraut werden, weil die Systemzeit in den meisten Betriebssystemen beliebig verändert werden kann. Auch nach dem Widerruf eines Zertifikates kann daher durch Rückdatierung des eingesetzten Computersystems mit dem zugehörigen Signierschlüssel noch ein Dokument signiert werden, das den Eindruck erweckt, während der Gültigkeitsdauer des Zertifikates entstanden zu sein.
Die Tatsache, dass eine digitale Signatur erst nach Ablauf der Gültigkeitsdauer oder nach der Revokation des Zertifikates entstanden ist, kann durch den Signierschlüsselinhaber naturgemäss kaum nachgewiesen werden. Aufgrund der Vermutung von Art. 17 Abs. 1 für den korrekten Einsatz des Signierschlüssels besteht daher die Gefahr, dass ein entsprechender Missbrauch durch den Signaturinhaber nicht nachgewiesen werden kann, und dass folglich eine aufgrund einer Schlüsselkompromittierung erfolgte Zertifikatsrevokation schlicht wirkungslos bleibt.
Um eine digitale Signatur zu überprüfen, muss anders als über die Systemzeit des Signiersystems festgestellt werden können, ob die Signatur wirklich bereits vor Ablauf der Gültigkeit bzw. vor dem Widerruf des eingesetzten Zertifikates existierte. Hierzu bedarf es einer (digitalen) Bestätigung durch einen vertrauenswürdigen Dritten (Zeitstempel).
Die einfachste Lösung dieses u.E. sehr schwerwiegenden Problems liegt darin, die Beweislast dafür, dass der Signierschlüssel noch während der Gültigkeitsdauer des Zertifikates zum Einsatz kam, beim auf die Signatur vertrauenden Dritten zu belassen. Denn im Gegensatz zum Signierschlüsselinhaber kann dieser den Gültigkeitsnachweis durch Anbringen eines Zeitstempels sehr einfach führen. Zudem sollte es im Ermessen des Dritten liegen, ob er einen – wohl regelmässig kostenpflichtigen – Zeitstempel aufbringen möchte, oder ob er die beweismässige Unsicherheit akzeptieren will.
Daraus ergibt sich der folgende Änderungsvorschlag für Art. 17 Abs. 1:
„*[1]Die Person, die behauptet, ihr Signierschlüssel sei ohne ihren Willen zum Einsatz gelangt, ist dafür beweispflichtig, sofern die Person, welche die digitale Signatur zu ihren Gunsten anführt, beweist, dass diese bereits vor Ablauf der Gültigkeitsfrist und vor einem Widerruf des Zertifikates existierte“.*

SBV S'agissant de la responsabilité du titulaire de la clé privée, il y a lieu de signaler deux points sur lesquels la loi devrait être modifiée:
Les questions de responsabilité peuvent être appréciées en fonction de la sphère d'influence respective des parties („Sphärentheorie“). Le titulaire de la clé privée devrait ainsi répondre de l'ensemble des faits se produisant dans sa propre sphère d'influence. En raison du renversement du fardeau de la preuve

statué à l'art. 17 al. 1, il doit en particulier apporter la preuve que „sa clé privée a été utilisée sans son consentement“. L'étendue de la preuve à fournir par le titulaire de la clé privée pourrait être précisée dans le sens suivant: a) ni le titulaire de la clé privée ni un fondé de procuration désigné par lui ou encore une personne de son entourage n'ont, dans le cas d'espèce, utilisé la clé; b) il a conservé la clé - de même que le matériel informatique nécessaire à son utilisation - avec la diligence requise.

En cas de manquement à ses obligations, la responsabilité du titulaire de la clé privée ne devrait pas se limiter à la couverture du dommage occasionné (intérêt négatif). Par analogie avec la représentation apparente („Anscheinvollmacht“) ou avec les clauses de légitimation utilisées en droit des papiers-valeurs, la transaction conclue au moyen d'une signature électronique devrait pleinement déployer ses effets sur le plan juridique. Cela présuppose néanmoins que le cocontractant se soit fié de bonne foi à un certificat valable. Les constatations faites ci-dessus ne se limitent pas à la conclusion d'un contrat, mais s'étendent également aux déclarations de volonté susceptibles de déployer des effets juridiques.

Nous proposons dès lors de modifier comme suit l'art. 17 :

Al. 1: „Il appartient à la personne qui affirme que sa clé privée a été utilisée sans son consentement d'en apporter la preuve. *Elle doit en particulier prouver, d'une part, que les obligations de diligence ressortissant au commerce électronique et à la conservation de la clé privée ont été observées et, d'autre part, qu'elle-même, un de ses fondés de procuration ou encore une personne de son entourage immédiat ne se sont pas servis de la clé privée*“.

Abs. 1 : „Die Person, die behauptet, ihr privater Signaturschlüssel sei ohne ihren Willen zum Einsatz gelangt, ist dafür beweispflichtig. *Sie hat insbesondere zu beweisen, dass einerseits den Sorgfaltspflichten im elektronischen Geschäftsverkehr und in bezug auf den privaten Signaturschlüssel nachgekommen wurde, andererseits dass weder sie, einer ihrer Bevollmächtigten, noch eine andere Person aus ihrem unmittelbaren Beziehungsnetz gehandelt hat.*“

Al. 2: *„Si les faits énoncés à l'alinéa 1 ne peuvent pas être entièrement prouvés et qu'un tiers s'est fié à un certificat valable, le titulaire de la clé privée se verra attribuer le contenu signé“.*

Abs. 2: „Kann der Beweis nach Abs. 1 nicht vollständig erbracht werden, und hat sich eine Drittperson gutgläubig auf das gültige Zertifikat verlassen, hat sich der Inhaber des privaten Signaturschlüssels den signierten Inhalt zurechnen zu lassen.“

Al. 3: *„Si les faits énoncés à l'alinéa 1 peuvent être entièrement prouvés, le titulaire de la clé privée ne se verra pas attribuer le contenu signé. Dans ce cas, la bonne foi du tiers dans le certificat valable ne sera pas protégée.“*

Abs. 3: „Kann der Beweis nach Abs 1 vollständig erbracht werden, hat sich der Inhaber des privaten Signaturschlüssels den signierten Inhalt nicht zurechnen zu lassen. Die Gutgläubigkeit der Drittperson in das gültige Zertifikat findet in diesem Fall keinen Schutz.“.

SIK Mühe haben wir mit der Umkehr der Beweislast nach Art. 17, weil wir den Eindruck haben, es sei ein wesentliches Hemmnis für die Einführung der elektronischen Signatur für den privaten Gebrauch, folglich auch für e-gov-Anwendungen (wenn die Bürger gegenüber der elektronischen Signatur zurückhaltend sind, werden sie weniger Gebrauch von diesen Anwendungen machen). Zu diesem Punkt meint einer unserer Delegierten:

„Die heutigen EDV-Systeme (PC, Betriebssysteme, Applikationen) sind noch so fehlerbehaftet, dass der private Benutzer der digitalen Unterschrift nicht das notwendige Fachwissen hat, seinen PC so einbruchssicher zu betreiben, dass die digitale Unterschrift von seinem PC nicht entwendet werden kann.
Falls die Umkehr der Beweislast erfolgt, ist die Akzeptanz dieser digitalen Unterschrift im Privatgebrauch nicht als hoch einzustufen, da das Risiko der Haftung unbekannt hoch ist. Sie dürfte fast so hoch sein, wie die Gefahren, welche von Wechseln ausgehen. Bei der Einführung der Kreditkarten haben die Banken bewusst die Abwicklung so konzipiert, dass bei den Benutzern eine hohe Akzeptanz eintritt und das neue Medium Kreditkarte ein Erfolg wird."
Der Wortlaut des Art. 17 und seines Kommentars sind u. E. auf alle Fälle nicht eindeutig genug. Auf einer Seite muss ein Inhaber nach Absatz 1 beweisen, dass sein Zertifikat ohne seinen Willen verwendet worden ist, auf der anderen Seite haftet er, nach Absatz 3, nur wenn man ihm vorwerfen kann (Um-Umkehr der Beweislast?), „die Massnahmen zur Geheimhaltung nicht beachtet zu haben (nach Art. 16 Abs. 2)". Technisch gesehen muss man im Übrigen grosse Schwierigkeiten bei der praktischen Anwendung dieses Art. 16 Abs. 2 erwarten: Wer wird eindeutig bestimmen können, welche exakten Vorkehrungen bei so komplexen Systemen zumutbar sind?
Wir kommen somit zur Meinung, dass eine Überprüfung des ganzen Art. 17 - evtl. auch Art. 16 - und deren Kommentare für eine ausgewogenere und eindeutigere Verteilung der Risiken unentbehrlich ist. Der publizierte Einwand des Kantons BL, die Weitergabe des Zertifikats sei zu verbieten, könnte dabei berücksichtigt werden (Beweispflichts- und Haftungsbestimmungen entsprechen schon einem praktischen Verbot, genügen jedoch vielleicht nicht).

SVV Abs. 2: Der Inhaber oder die Inhaberin des privaten Signaturschlüssels haftet der Drittperson für Schäden, die diese deswegen erleidet, weil sie sich *gutgläubig* auf das gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten verlassen hat.
Begründung: Wie bereits einführend zu den Haftungsbestimmungen erwähnt, sind diese in unseren Augen ausgewogen auf die verschiedenen Parteien verteilt. Insofern ist an der Bestimmung von Art. 17 Abs. 2 nichts abzuändern. Wenn das Wort „verlassen" auch bereits eine Gutgläubigkeit impliziert, so beantragen wir der Klarheit halber dennoch im Artikel auf die Gutgläubigkeit hinzuweisen.
Abs. 3: Die Haftung entfällt, wenn der Inhaber oder die Inhaberin des privaten Signaturschlüssels die Vorkehrungen *nach diesem Gesetz und den dazugehörigen Ausführungsbestimmungen getroffen hat. Im Übrigen gelten die Bestimmungen des Obligationenrechts.*
Begründung: In Art. 10 Abs. 2 haben wir beantragt, dass die Sorgfaltspflichten im Gesetz selbst resp. durch den Bundesrat in den Ausführungsvorschriften erwähnt werden. Der Artikel steht in einer engen Beziehung zu Art. 16 Abs. 2. Es rechtfertigt sich folglich, in Art. 17 Abs. 3 über Art. 16 hinaus auf das ganze BGES und die entsprechenden Ausführungsbestimmungen zu verweisen.
Im zweiten Satz der Bestimmung wird schliesslich auf die Stellvertretungsregeln des OR verwiesen. Auch hier sind wir der Meinung, dass dieser Verweis zu eng gefasst ist. So können sich beim Fremdeinsatz eines Signaturschlüssels auch Fragen aus anderen Gebieten des OR stellen (Willensmängel, unerlaubte Handlung, Geschäftsführung ohne Auftrag etc.). Wir beantragen deshalb, den Verweis auf das ganze OR auszudehnen.

SWICO Ist der Verweis auf das Stellvertretungsrecht angebracht? Sicherlich nicht, was die Nennung im Gesetzestext anbetrifft; andererseits kann es für gewisse Gedankenspiele hilfreich sein, wobei die Anscheinsvollmacht und Blankovollmacht bei diesen elektronischen Systemen besser passt (vgl. Die Stellvertretung ohne Ermächtigung, Diss. 1987, Georges Violand).

Man sollte hier wohl die Sphärentheorie in aller Konsequenz im Gesetz aufnehmen.

Die Verantwortung für den privaten Signaturschlüssel kann sich nur auf den direkt beeinflussbaren Bereich beziehen. Dies wiederum bedeutet, dass der Anbieter von Zertifizierungsdiensten (oder der Service Provider) eine entsprechend gesicherte Umgebung zur Verfügung stellt. Dies kann aus technischer Sicht z.B. kein Standard PC sein (vergleiche zum Ganzen §17 deutsches SigG).

Zusammenfassend sei darauf hingewiesen, dass man sich bewusst sein sollte, dass es vorliegend eine völlig neue Sachlage zu beurteilen/zu regeln gilt, die es rechtfertigt, unabhängig von gegebenen Lösungen eine eigenständige Regelung zu finden. Damit stellt sich die Frage, ob nicht die Regelung einer Legitimationsklausel in Analogie zum Wertpapier sich rechtfertigen würde. Denn es werden sehr hohe Sicherheitsanforderungen gesetzt, verbunden mit einer „Entpersonalisierung" - d.h. Loslösung vom persönlichen Kontakt und gegenseitigen Vertrauen in ein (technisches) Hilfsmittel. Konsequenterweise sollte (wie z.B. im Checkrecht - mit formeller Checkstrenge) der erforderliche gute Glaube geschützt werden, werden doch hier wie dort allein formelle/sachliche Kriterien geprüft, um über Rechtmässigkeit und Rechtswirkung (einer Willenskundgabe) entscheiden zu können/dürfen. - Mit anderen Worten wäre die gesetzliche Schaffung einer Legitimationsklausel (entsprechend OR Art. 976 - siehe Kleiner in Festschrift Max Keller, 1989, S. 723 f) wohl mehr als nur gerechtfertigt.

Abs. 1: Es muss mit Nachdruck darauf hingewiesen werden, dass die Regelung der Beweislastumkehr ein „must" für die Akzeptanz des Signaturgesetzes in der Wirtschaft sein dürfte.

Sodann müsste der Beweisinhalt wohl etwas genauer umschrieben werden, er bezieht sich u.E. einerseits darauf, (i)dass weder er als Inhaber noch ein Bevollmächtigter oder eine Person aus seinem Beziehungsnetz gehandelt hat - sondern irgendein Dritter -, andererseits, dass er seinen Sorgfaltspflichten im Umgang mit dem privaten Signaturschlüssel und seinen elektronischen Equipments gewahrt hat.

Abs. 2: U.E. darf es nicht sein, dass hier nur für Schaden (negatives Vertragsinteresse) gehaftet wird; vielmehr müsste das Rechtsgeschäft zustande kommen bzw. die übermittelten Daten seine Rechtswirkung entfalten (so z.B. der Fall eines Börsengeschäftes, bei dem sich der Kurs extrem vom Kaufpreis weg entwickelt. - Warum wird hier also nicht der Ansatz der Anscheinsvollmacht gemacht (so auch D. Rosenthal) bzw. vom Gesetzgeber in den Erläuterungen diese ohne plausible Begründung verworfen (zwar handelt es sich klar nicht um eine Stellvertretung - und damit unpassend -, doch wäre jene Lösung durchaus auch als Gedankenspiel für etwas neues möglich)? Auch wäre hier der Ansatz einer Legitimationsklausel im vorerwähnten Sinne ein denkbarer und durchaus sachgerechter Ansatz.

Denn der Inhaber von Zertifikaten hat es ja in der Hand, eine Nutzungsbeschränkung vorzusehen (Sofern dies mit Attributen umgesetzt wird. Dazu gehört dann auch die zwingende Prüfungspflicht durch die Relying Party). Aus-

serdem liegt es allein im Wille des Inhabers, sich den Weg über die elektronische Signatur zu öffnen.
Auch wenn diese Bestimmungen allein für digitale Signaturen mit entsprechenden elektronischen Zertifikaten formalrechtlich gelten (so Geltungsbereich des BGES), so ist wohl zu befürchten, dass der Richter diese Haftungsbestimmungen analog auch für andere vergleichbare Sachverhalte anwendet oder mindestens seine Meinungsbildung hiervon mit beeinflussen lassen wird.
Abs. 3: Diese Bestimmung muss derart präzisierend umformuliert werden, dass diese Haftungsregelung nur zur Anwendung kommt, wenn kumulativ vom Schlüsselinhaber bewiesen werden kann, dass (i)er die entsprechenden Sorgfaltspflichten eingehalten hat und (ii)er nicht die Person war, die gehandelt hat, sowenig wie eine von ihm ermächtigte Drittperson (bzw. früher einmal ermächtigte Drittperson). Hier sieht man auch, weshalb es von grösster Bedeutung ist, dass die Bestimmung von Art. 10 Abs. 2 und Art. 16 Abs. 2 näher spezifiziert wird.
Wir fragen uns, ob der letzte Satz „Im übrigen …“ nicht gestrichen werden müsste, ist er doch sachfremd. So sagen ja die Erläuterungen in anderem Zusammenhang, dass das elektronische Zertifikat die Vollmacht als solches nicht ersetze.
Vorschlag zu Korrekturen des Gesetzeswortlautes (kursive Textstellen sollen eingefügt werden):
Abs. 1: „Die Person, die behauptet, ihr privater Signaturschlüssel sei ohne ihren Willen zum Einsatz gelangt, ist dafür beweispflichtig. *Sie hat insbesondere zu beweisen, dass einerseits den Sorgfaltspflichten* (hier könnte ein Verweis auf die einschlägigen Bestimmungen vorgenommen werden) *im elektronischen Geschäftsverkehr und in Bezug auf den privaten Signaturschlüssel nachgekommen wurde, andererseits dass weder sie, einer ihrer Bevollmächtigter, noch eine Person aus ihrem unmittelbaren Beziehungsnetz* (dabei wird etwa an den gemeinsamen Haushalt sowie an den Arbeitsplatz gedacht) *gehandelt hat.*“
Abs. 2: *„Kann der Beweis nach Abs 1 nicht vollständig erbracht werden, und hat sich die Drittperson gutgläubig auf eine gültige digitale Signatur im Zusammenhang mit einem gültigen Zertifikat verlassen, hat sich der Inhaber des privaten Signaturschlüssels den signierten Inhalt zurechnen zu lassen.“*
Abs. 3: *„Kann der Beweis nach Abs. 1 vollständig erbracht werden, hat sich der Inhaber des privaten Signaturschlüssels den signierten Inhalt nicht zurechnen zu lassen. Die Gutgläubigkeit der Drittperson in das gültige Zertifikat finden keinen Schutz. „*
Sollte man sich zur Einführung einer Legitimationsklausel durchringen, so könnte die Bestimmung von Art. 17 wie folgt lauten:
„[1]Stützt sich eine Drittperson (Empfänger) gutgläubig auf ein gültiges Zertifikat und ist die Prüfung der digitalen Signatur und des Zertifikates systemmässig fehlerfrei erfolgt (Legitimationsprüfung), hat sich der Inhaber des privaten Signaturschlüssels den signierten Inhalt zurechnen zu lassen.
[2]Ist die Prüfung nicht systemmässig fehlerfrei erfolgt und behauptet der Inhaber, sein privater Signaturschlüssel sei ohne sein Willen zum Einsatz gelangt, ist er dafür beweispflichtig. Er hat insbesondere zu beweisen, dass einerseits den Sorgfaltspflichten im elektronischen Geschäftsverkehr und in Bezug des privaten Signaturschlüssel nachgekommen wurde, andererseits dass weder er, einer seiner Bevollmächtigter, noch eine Person aus seinem unmittelbaren Beziehungsnetz gehandelt hat.

[3]Kann der Beweis nach Abs. 2 nicht vollständig erbracht werden, haftet der Inhaber des privaten Signaturschlüssels für Schäden, die deswegen die Drittperson erleidet."

TSM Art. 17 regelt die Haftung des Inhabers oder der Inhaberin des privaten Schlüssels. Abs. 1 und 2 beinhalten eine Beweislastumkehr, welche die Person, die behauptet, dass ihr privater Signaturschlüssel ohne ihren Willen gebraucht worden sei, beweis- und schadenersatzpflichtig macht. Diese Regelung ist gut wegen der Stärkung der an sich schwächeren Position des Empfängers und auch im Interesse des sicheren Geschäftsverkehrs.

Für die TSM ist es wichtig, dass sie sich nicht nur faktisch, sondern auch juristisch absichern kann. Dies gilt insbesondere auch für den Fall, dass die elektronische Signatur durch den Absender (also den Inhaber des privaten Signaturschlüssels) oder durch Dritte missbraucht wird. In diesen Fällen ist es wichtig, dass die Verantwortung für das fehlbare Verhalten nicht der TSM auferlegt werden kann, sondern dass diejenigen, die die Signatur unrechtmässig benutzt haben, die Konsequenzen ihres Handelns tragen müssen.

Vischer Der in Art. 17 Abs. 3 Satz 2 enthaltene Verweis auf die Art. 38 und 39 OR ist zu ersetzen durch einen Verweis auf die allgemeinen Bestimmungen über die unerlaubte Handlung (Art. 41 ff. OR). Es ist im Gesetz ausdrücklich festzulegen, wer für das Tun oder Unterlassen des Signaturschlüsselinhabers im Sinne von Art. 17 Abs. 3 beweispflichtig ist.

Die grösste mit dem vorliegenden Gesetzesentwurf verbundene rechtliche Schwierigkeit liegt zweifellos darin, dass die Rechtsfolgen der unbefugten Verwendung eines fremden Signaturschlüssels definiert werden müssen.

Der Gesetzesentwurf sagt zunächst, dass der Inhaber eines Signaturschlüssels sich jede Verwendung dieses Schlüssels entgegenhalten lassen muss, es sei denn, er beweise, dass der Signaturschlüssel ohne seinen Willen zum Einsatz gelangt ist (Art. 17 Abs. 1). Damit wird eine gesetzliche Vermutung dafür geschaffen, dass die erfolgte Verwendung eines Signaturschlüssels vom Willen des Schlüsselinhabers gedeckt ist. Im Interesse der Sicherheit und Zuverlässigkeit des Rechtsverkehrs mag diese Regelung zu begrüssen sein. Es darf jedoch nicht übersehen werden, dass ein allfälliger Missbrauch des Signaturschlüssels durch Unbefugte äusserst schwierig zu beweisen sein wird. Der Schlüsselinhaber wird dadurch unter Umständen in die Situation versetzt, Verpflichtungen erfüllen zu müssen, die er nie eingehen wollte.

Sofern der Schlüsselinhaber den Missbrauchsbeweis erbringen kann, muss er sich die entsprechende" digital signierte Erklärung nicht entgegenhalten lassen. Immerhin haftet er aber im Umfang des negativen Vertragsinteresses für den Schaden des gutgläubigen Dritten, sofern er nicht „alle nach den Umständen zumutbaren Vorkehrungen" getroffen hat, um den Schlüssel so aufzubewahren, „dass eine Verwendung durch unbefugte Drittpersonen ausgeschlossen werden kann" (Art. 17 Abs. 3 i. V. m. Art. 16 Abs. 2). Der Gesetzesentwurf sagt nicht ausdrücklich, wer in diesem Zusammenhang für das Tun oder Unterlassen des Signaturschlüsselinhabers beweispflichtig ist. Es ist anzunehmen, dass die Beweislast beim Schlüsselinhaber liegen soll; Art. 17 Abs. 3 will wohl dem Schlüsselinhaber die Möglichkeit geben, den Exkulpationsbeweis zu führen. Diese Beweislastverteilung sollte im Gesetz ausdrücklich erwähnt werden.

Ob die rechtliche Situation des Signaturschlüsselinhabers damit eine befriedigende ist, ist letztlich eine Wertungsfrage. Die vorgeschlagene gesetzliche Regelung führt dazu, dass ein Schlüsselinhaber sich mit eigener Unsorgfalt in erhebliche, ja vernichtende Schwierigkeiten bringen kann. Ob die mit dem In-

strument der elektronischen Signatur verbundenen volkswirtschaftlichen Vorteile dieses Risiko rechtfertigen, müssen die politischen Instanzen entscheiden.
Schliesslich ist anzumerken, dass es sich bei der Verwendung fremder Signaturschlüssel nicht um einen Tatbestand des Stellvertretungsrechts handelt, weil der Täter nicht in fremdem Namen, sondern unter fremdem Namen auftritt. Der in Art. 17 Abs. 3 Satz 2 enthaltene Verweis auf die Art. 38 und 39 OR ist deshalb nicht sachgerecht. In zivilrechtlicher Hinsicht sind stattdessen die allgemeinen Bestimmungen über die unerlaubte Handlung (Art. 41 ff. OR) anwendbar.

VSG Buona strutturazione delle responsabilità del detentore di una chiave privata e dei fornitori di certificazioni (art. 17). Il titolare di una chiave privata risponderà in virtù del contratto solo se vi ha acconsentito. Il terzo che ha fatto affidamento su un certificato beneficia dell'inversione dell'onere probatorio (il titolare della chiave privata deve provare che la stessa è stata utilizzata contro la sua volontà: se non è in grado di fornire tale prova, si applicano le norme sulla conclusione del contratto). Se il titolare riesce a discolparsi (art. 16 e 17 cpv. 3), subentrano gli art. 38 e 39 CO.
Opportuno forse rendere ancora più trasparenti i diversi gradi e concetti di responsabilità. In particolare per il titolare della chiave privata.

VSW Eine digitale Signatur ist keine persönliche Unterschrift wie eine Unterschrift von Hand. Anders als letztere ist eine digitale Signatur faktisch übertragbar, weil alles, was es zu deren Erzeugung braucht, eine Zahlenkombination ist. Wenn deshalb der Besitzer seinen privaten Schlüssel nicht geheim hält und ein Dritter diesen benutzt, so liegt ein Fall der Stellvertretung im Sinne von Art. 32 ff. OR vor: die unbefugtermassen digital signierende Person verpflichtet nicht sich selber, sondern die Inhaberin des privaten Schlüssels. Letztere muss diesfalls nur dann für die Vertragserklärung einstehen, wenn sie dieser vorgängig oder nachträglich zustimmt. Wenn sie jedoch die Zustimmung verweigert, ist der Vertrag nicht zustande gekommen. Auch wenn in diesem Fall dem Empfänger der digital signierten Erklärung gegen die Inhaberin des privaten Schlüssels aus Art. 17 Abs. 2 oder gegen die unbefugtermassen digital signierende Person aus Art. 39 OR Schadenersatzansprüche zustehen, und auch wenn die Inhaberin des privaten Schlüssels gemäss Art. 17 Abs. 1 die Beweislast trägt, dass dieser gegen ihren Willen verwendet worden ist, so ist doch festzustellen, dass digital signierte Vertragserklärungen gegenüber herkömmlich signierten Vertragserklärungen ein zusätzliches Fehlerpotential enthalten.
Durch diese Lösung wird der rechtspolitische Entscheid, wer das Risiko des Missbrauches digitaler Signaturen zu tragen hat, tendenziell zulasten der Wirtschaft (Anbieter von Gütern und Dienstleistungen) und zu Gunsten der Konsumenten (Nachfrager von Gütern und Dienstleistungen) gelöst. Wir befürworten eine Lösung, mit der die gegenteilige Risikoverteilung vorgenommen wird.

321.18 Art. 18

Kantone / Cantons / Cantoni

BE Ohne ausführende Erläuterungen ist Abs. 3 nicht ohne weiteres verständlich, da in Art. 8 Abs. 1 lit. c von Nutzungsbeschränkungen und im Gegenzug dazu in Art. 18 Abs. 3 von Haftungsbeschränkungen gesprochen wird. Der Zusammenhang zwischen Haftungs- und Nutzungsbeschränkungen ist nicht ohne weiteres ersichtlich. Im Sinne einer konsumenten- bzw. leserfreundlichen Gesetzesredigierung müsste klarer zum Ausdruck kommen, dass der Anbieter von

Zertifizierungsdiensten nur im Rahmen der zugelassenen Nutzung haftet - z.B. bis zu einem festgesetzten Maximalbetrag.

BS Unter Ziff. 210.073 äussert sich der Begleitbericht auf Seite 24 über die Wegbedingung der Haftung in den übrigen Fällen, wobei die übrigen Fälle die nicht anerkannten Anbieterinnen von Zertifizierungsdiensten betreffen, nämlich die Zertifizierungsdiensteanbieter. Diese sind aber gerade nicht - wie es auf der zweituntersten Zeile heisst - anerkannt.

JU Le Gouvernement de la République et Canton du Jura approuve le principe du renversement du fardeau de la preuve tel qu'il résulte de l'alinéa 2 du projet.

GE En ce qui concerne la responsabilité des fournisseurs de services de certification reconnus, l'art. 18 l'a définie de façon stricte puisqu'elle est engagée même en l'absence d'une quelconque faute. C'est la simple violation objective des devoirs imposés par la loi qui crée la responsabilité, ce qui est en soi un élément important contribuant à la confiance du public dans le système instauré.
Cette responsabilité est encore renforcée par le fait que l'art. 18, al. 3 prévoit que „les fournisseurs de services de certification reconnus ne peuvent exclure leur responsabilité découlant de la présente loi non plus que celle de leurs auxiliaires“ Ce principe est toutefois immédiatement anéanti par la deuxième phrase du même alinéa qui prévoit que sont réservées les limitations de responsabilité découlant du certificat lui-même.
Il est dès lors impératif que la loi fixe très précisément les limites admissibles à cette restriction de responsabilité figurant sur le certificat lui-même, à défaut de quoi, c'est toute la réglementation de la responsabilité stricte des fournisseurs de services de certificat, voulue par l'art. 18, qui risque d'être contournée par ce biais.

TI Lo scrivente Consiglio concorda con la formulazione dell'art. 18 cpv. 3, che impedisce al prestatore di servizi di certificazione di escludere le proprie responsabilità.

Parteien / Partis / Partiti

PLS L'art. 18 devrait clairement faire ressortir le caractère causal (indépendant de toute faute) de la responsabilité des fournisseurs de services de certification.

Organisationen / Organisations / Organizzazioni

camera commercio Comprensibilmente, il cpv. 2 prevede il rovesciamento dell'onere della prova per i prestatori di servizi di certificazione, poiché chi è danneggiato dall'uso di un certificato ben difficilmente può provare la responsabilità del prestatore di servizi. E' tuttavia importante dare al prestatore di servizi di certificazione la possibilità di discolparsi. Sono semplicemente inaccettabili condizioni che comportano la responsabilità dei prestatori di servizi indipendentemente da una qualsiasi colpa, visto che ciò escluderebbe ogni possibilità di copertura assicurativa. Siamo dell'opinione che una simile richiesta rappresenti un ostacolo insormontabile per un prestatore di servizi privato, nell'ottica di un riconoscimento del suo servizio.

Clusis La question de la responsabilité des fournisseurs de services de certification est réglée à l'art. 18, dont l'al. 1 exprime le principe d'une responsabilité pour le dommage causé aux titulaires de clés privées ainsi qu'aux tiers qui se sont fiés aux certificats, „lorsqu'ils violent des obligations que leur impose la présente loi et ses dispositions d'exécution pertinentes“. L'al. 2 prévoit encore qu'il appartiendra à ces fournisseurs de services de certification d'apporter la preuve du respect de ces obligations.

Il faut donc noter que cette responsabilité de l'autorité de certification est engagée même en l'absence d'une quelconque faute, c'est-à-dire même en cas de violation non fautive des devoirs imposés par la loi, au premier rang desquels figurent celui d'annuler immédiatement un certificat électronique si la personne qui le demande est légitimée à le faire (art. 11).

Une responsabilité stricte est certainement dictée par le souci, exprimé à l'art. 1, al. 2 let. a „promouvoir la fourniture de services de certification électronique sur un large public". Par ailleurs, l'art. 18 al. 3 prévoit encore que „les fournisseurs de services de certification reconnus ne peuvent exclure leur responsabilité découlant de la présente loi non plus que celle de leurs auxiliaires".

Cependant, cette prohibition d'exclusion de responsabilité est fortement mise à mal par la deuxième phrase de l'art. 18 al. 3, qui prévoit que sont réservées les limitations de responsabilité découlant du certificat lui-même. Il est ici fait référence à l'art. 8 alinéa 1 let. c, qui autorise la mention sur le certificat d'éventuelles „limites fixées à son utilisation".

Il est probable qu'au plan pratique, il sera extrêmement difficile de distinguer entre la licéité des limitations de responsabilité portant sur l'utilisation du certificat et l'interdiction de limiter sa responsabilité contenue à l'art. 18. Concrètement, les fournisseurs de services de certification seront certainement tentés de recourir à une formulation très large sur le certificat lui-même tout en se retranchant derrière la possibilité offerte à la deuxième phrase de l'art. 18 al. 3.

DigiSigna Wie / Comme / Come camera commercio.

Distefora Verschiedene Stimmen, insbesondere Anbieterinnen von Zertifizierungsdiensten, haben aus naheliegenden Gründen die in Art. 18 vorgesehene Kausalhaftung kritisiert. Wir können uns dieser Kritik nicht anschliessen. Die Kausalhaftung stellt eine klare Zuordnung der Verantwortlichkeit sicher und ist auch sachgerecht. Die Anbieterinnen von Zertifizierungsdiensten haben durch diese Kausalhaftung ein direktes, immanentes Interesse an der Einhaltung ihrer Pflichten gemäss BGES, was sicherlich zu einer erhöhten Sicherheit beim Einsatz der elektronischen Signatur führen wird. Diese interessengerechte Haftungszuordnung wird auch zu einer erhöhten Akzeptanz des E-Business beim Nutzer führen und ist geeignet, den heute noch landläufig verbreiteten Befürchtungen betreffend die Missbrauchsgefahren und der damit verbundenen Zurückhaltung der Nutzer gegenüber den elektronischen Vertriebswegen Einhalt zu gebieten. Die Bestimmung setzt damit ein klares Zeichen für eine erhöhte Sicherheit und Akzeptanz des elektronischen Geschäftsverkehrs, was im Hinblick auf ein nachhaltiges Wachstum des E-Business selbstredend von entscheidender Bedeutung ist. Die vorgesehene Kausalhaftung steht demnach im Interesse der schweizerischen Wirtschaft.

economiesuisse Zunächst erscheint es uns betreffend Abs. 1 empfehlenswert, auf die Kausalhaftung des Zertifizierungsdienstanbieters für die korrekte Erstellung und Administration der Zertifikate noch klarer hinzuweisen:

„[1]Die anerkannten Anbieterinnen von Zertifizierungsdiensten haften ungeachtet eines Verschuldens dem Inhaber oder der Inhaberin (…)".

Satz 1 von Abs. 3 stellt zunächst fest, dass die Anbieterinnen von Zertifizierungsdiensten „ihre Haftung aus diesem Gesetz weder für sich noch für Hilfspersonen wegbedingen" können. Unmittelbar anschliessend wird festgestellt, dass „Haftungsbeschränkungen, die sich aus dem Zertifikat (Art. 8 (1) lit. c) ergeben, vorbehalten" bleiben. Hierbei muss es sich unseres Erachtens um eine redaktionell missglückte Formulierung handeln, ist doch die „Nutzungsbeschränkung" im Zertifikat das entscheidende Element (Unterbleiben der An-

zeige im Zertifikat, fehlerhafte Anzeige der Beschränkung, Missachtung der Beschränkung).

Denn der Hinweis auf Art. 8 (1) lit. c lässt unseres Erachtens allein diese Interpretation zu. Ein Hinweis auf die fehlende Haftung der Diensteanbieter für die Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung durch den Empfänger der elektronisch versandten Mitteilung (Drittperson) wäre grundsätzlich aber überflüssig, da insoweit eine Verpflichtung des Diensteanbieters „aus diesem Gesetz“ nicht besteht.

Soll dieser Aspekt aber trotzdem im Gesetz festgeschrieben werden, schlagen wir den nachfolgenden, präziseren Wortlaut von Abs. 3 vor:

„[3]Die anerkannten Anbieterinnen von Zertifizierungsdiensten können ihre Haftung für Verpflichtungen, die sich aus diesem Gesetz ergeben, einschliesslich derjenigen für die Erfüllung dieser Verpflichtungen durch Hilfspersonen weder vollständig ausschliessen noch nach Art oder Umfang einschränken. Sie haften jedoch nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung ergeben, soweit diese bei ordnungsgemässer Anwendung unmittelbar aus dem Zertifikat ersichtlich war."

Zulässige Nutzungsbeschränkungen müssen in den Ausführungsvorschriften näher spezifiziert werden (z.B. analog der handelsrechtlichen Vollmacht). Jedenfalls muss die Überprüfung von Nutzungsbeschränkungen ohne grossen Aufwand maschinell möglich sein, da sonst derartige Zertifikate im wirtschaftlichen Verkehr kaum akzeptiert würden.

FGSec Welche Haftung tragen die Anerkennungsstellen?

Jeune Barreau vaudois L'art. 18 al. 1 du Projet dégage le principe d'une responsabilité des fournisseurs de services de certification reconnus pour le dommage causé aux titulaires de clés privées ainsi qu'aux tiers qui se sont fiés aux certificats, „lorsqu'ils violent des obligations que leur impose la présente loi et ses dispositions d'exécution pertinentes“. L'al. 2 prévoit encore qu'il appartiendra à ces fournisseurs de services de certification d'apporter la preuve du respect de ces obligations.

Ainsi, la responsabilité de l'autorité de certification est engagée même en l'absence d'une quelconque faute, c'est-à-dire même en cas de violation non fautive des devoirs imposés par la loi, au premier rang desquels figurent celui d'annuler immédiatement un certificat électronique si la personne qui le demande est légitimée à le faire (art. 11).

De plus, l'art. 18 al. 3 prévoit encore que „les fournisseurs de services de certification reconnus ne peuvent exclure leur responsabilité découlant de la présente loi non plus que celle de leurs auxiliaires“.

Toutefois, l'art. 18 al. 3 prévoit que „sont réservées les limitations de responsabilité découlant du certificat lui-même. Il est ici fait référence à l'art. 8 al. 1 let. c du Projet, qui autorise la mention sur le certificat d'éventuelles „limites fixées à son utilisation“, ce qui relativise la portée de l'exclusion de responsabilité.

Dans les faits, les fournisseurs de services de certification risquent de recourir à une formulation très large sur le certificat lui-même afin de limiter leur responsabilité.

kf Der Begriff Haftungsbeschränkungen verwirrt. Wir schlagen vor, gemäss Art. 8 Abs. 1 Bst. c auch hier von Nutzungsbedingungen zu sprechen.

Rosenthal Zur vorgeschlagenen Haftung der Anbieter von Zertifizierungsdiensten soll an dieser Stelle nur eine gesetzestechnische Bemerkung gemacht werden und der Artikel nicht im Einzelnen analysiert oder bewertet werden.

Die Verfasser des BGES-VE gehen davon aus (Erläuterungen, Nr. 210.073), dass Art. 18 eine Kausalhaftung der Zertifizierungsdienstanbieter begründet. Soll dem tatsächlich so sein, so muss der betreffende Artikel umformuliert werden.

Wird Art. 18 streng beurteilt, stellt er keine genügende Anspruchsgrundlage für Schadenersatz dar. Die Norm hält lediglich fest, dass der Zertifizierungsdienstanbieter „haften“ soll. Von einem Ersatz eines Schadens ist nicht die Rede. Es liegt mithin eine ähnliche Situation wie im Falle von Art. 321e OR vor: Auch dort ist davon die Rede, dass ein Arbeitnehmer „für den Schaden verantwortlich“ sei, den er dem Arbeitgeber zufüge. Dennoch ist die Anspruchsgrundlage in einem Schadenersatzprozess nicht Art. 321e OR, sondern Art. 97 Abs. 1 OR.

Schadenersatz kann gegenüber den Zertifizierungsdienstanbietern zwar gefordert werden. Will ein Geschädigter dies tun, wird er seinen Anspruch aber auf Art. 41 Abs. 1 OR abstützen müssen und diese Anspruchsnorm in Verbindung mit Art. 18 anrufen. Art. 18 kommt dabei mit Art. 16 Abs. 2 die Rolle der „Schutznorm“ zu, die gemäss Art. 41 Abs. 1 OR verletzt sein muss (Kriterium der Widerrechtlichkeit), soll der Geschädigte den Ersatz seines Vermögensschadens erfolgreich geltend machen können. Das aber hätte zur Folge, dass ein Schadenersatzanspruch primär nach den herkömmlichen Regeln des Art. 41 Abs. 1 OR beurteilt werden müsste und der Geschädigte somit auch das Verschulden des Zertifizierungsdienstanbieters nachweisen müsste.

Zusammengefasst bedeutet dies, dass die jetzige Formulierung des Art. 18 Abs. 1 entgegen den Absichten bei genauer Anwendung keine Kausalhaftung zu begründen vermag. Zudem ist es der Geschädigte, der das Verschulden des Zertifizierungsdienstanbieters nachweisen muss (Die Beweislastregel des Art. 18 Abs. 2 betrifft nur die Erfüllung der Pflichten, d.h. das Element der Widerrechtlichkeit des Verhaltens). Auch das ist wohl nicht im Sinne der Verfasser des BGES-VE.

SAV La responsabilité propre du fournisseur de certification et de ses auxiliaires requiert des dispositions particulières sur la responsabilité, en particulier pour limiter strictement les cas d’exclusion de responsabilité. Il convient aussi d’empêcher les reports de responsabilité abusifs sur le titulaire suisse en cas de procès contre le fournisseur de certification à l’étranger, car cela pourrait priver le titulaire suisse de ses droits, notamment en matière de for. Ainsi par exemple, le client de Swisskey s’engage-t-il à indemniser Swisskey à tous égards si celle-ci se trouve impliquée dans un litige juridique entre le client et des tiers ou simplement incriminée par un tiers, donc même sans faute aucune du client de Swisskey. Cela peut être la ruine pour une petite entreprise qui devrait assumer la défense de Swisskey dans un procès aux USA.

Vgl. auch zu Art. 10 / Cf. également ad art. 10 / Cfr. anche ad art. 10.

SBV Dans l'exercice des obligations que leur impose la loi, les fournisseurs de services de certification assument une responsabilité causale. Nous proposons dès lors de modifier cette disposition comme suit:

Al. 1: „Les fournisseurs de services de certification reconnus répondent*, indépendamment de toute faute,* du dommage qu'ils causent au titulaire…“.

Abs. 1: „Die anerkannten Anbieterinnen von Zertifizierungsdiensten haften *ungeachtet eines Verschuldens* dem Inhaber ….“.

Par ailleurs, afin d'assurer l'uniformité de la terminologie utilisée dans la loi (cf. notamment art. 8 al. 1 lit. c), le terme „limitations de responsabilité“ figurant à l'art. 18 al. 3 devrait être remplacé par „*limitations à l'utilisation du certificat*“.

SWICO Aus Art. 17 ergibt sich die Pflicht der Anbieterin, für das Versagen ihrer Einrichtungen zu haften. Es ist sicher kritisch, wer beim Ausfall einer technischen Komponente haften muss, wenn keine Verletzung der Sorgfaltspflicht vorliegt. Hier kann man sich natürlich fragen, wer schlussendlich das Risiko tragen soll. Im deutschen SigG wird die Haftung klar der Anbieterin übertragen (§11 Abs. 1).

Abs. 1 ist der Klarheit halber mit „ungeachtet eines Verschuldens“ zu ergänzen: „Die anerkannten Anbieterinnen von Zertifizierungsdiensten haften *ungeachtet eines Verschuldens* dem Inhaber ….“.

Satz 1 von Abs. 3 stellt zunächst fest, dass die Anbieterin von Zertifizierungsdiensten ihre Haftung aus diesem Gesetz nicht wegbedingen könne. Anschliessend wird ausgeführt, dass „Haftungsbeschränkungen, die sich aus dem Zertifikat (Art. 8 Abs. 1 lit. c) ergeben, vorbehalten“ bleiben. Hierbei muss es sich unseres Erachtens um eine redaktionell missglückte Formulierung handeln, die zu Missinterpretationen Anlass geben dürfte. Denn es soll nicht eine Ausnahme der Haftungsbeschränkung statuiert werden, sondern vielmehr die Selbstverständlichkeit festgehalten werden, dass bei Fehlern in Zusammenhang mit der Anzeige von Nutzungsbeschränkungen im Zertifikat bzw. bei Missachtung von Nutzungsbeschränkungen sich die Haftung reduzieren bzw. gar entfallen könne. Eine solche Bestimmung wäre unseres Erachtens aber überflüssig; soll jedoch trotzdem daran festgehalten werden, schlagen wir folgenden präzisierenden Wortlaut in Abs. 3 vor: „... noch für Hilfspersonen wegbedingen. *Sie haften jedoch nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung (Art. 8 Abs. 1 lit. c) ergeben, soweit diese bei ordnungsgemässer Anwendung unmittelbar aus dem Zertifikat ersichtlich war*.“

SVV Abs. 3: „Die anerkannten Anbieterinnen von Zertifizierungsdiensten können ihre Haftung *für Verpflichtungen, die sich aus diesem Gesetz ergeben, einschliesslich derjenigen für die Erfüllung dieser Verpflichtungen durch Hilfspersonen weder vollständig ausschliessen noch nach Art oder Umfang einschränken*“.

Sie haften jedoch nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung (Art. 8 Abs. 1 lit. c) ergeben, soweit diese bei ordnungsgemässer Anwendung unmittelbar aus dem Zertifikat ersichtlich war.“

Begründung: In Satz 1 von Art. 18 Abs. 3 wird zunächst festgestellt, dass die Anbieterinnen von Zertifizierungsdiensten ihre Haftung aus diesem Gesetz weder für sich noch für Hilfspersonen wegbedingen können. Vorbehalten sind die Haftungsbeschränkungen, die sich aus dem Zertifikat ergeben.

Diese Formulierung erweckt den Eindruck, dass die Anbieterinnen von Zertifizierungsdiensten zwar keinen vollständigen Ausschluss ihrer Haftung vornehmen, aber eine Beschränkung ihrer Haftung vorsehen können, soweit sich eine solche Beschränkung aus dem Zertifikat selbst ergibt. Diese Interpretation wäre durchaus sachgerecht im Hinblick auf die differenzierte Ausgestaltung einzelner Zertifikate und ihre Verwendung in der Praxis. Der Verweis auf Art. 8 Abs. 1 lit. c scheint eine solche Interpretation aber auszuschliessen, weil darin auf die Nutzungsbeschränkungen eines Zertifikats verwiesen wird und damit nicht auf die eigentlichen Haftungsgrundlagen der Dienstanbieter, denn Nutzungsbeschränkungen im Sinne des Gesetzes sind auf die eigentliche Verwendung der elektronischen Signatur im Rahmen einzelner Rechtsgeschäfte ausgerichtet und gerade nicht auf die Verpflichtungen der Dienstleistungsanbieter

bezogen. Dennoch scheint die Bestimmung eine inhaltliche Beschränkung der Nutzung des Zertifikats mit der Haftung für Fehler im Rahmen der Ausstellung oder Betreuung zu verbinden. Diese beiden Punkte sind aber streng zu trennen und unterschiedlich zu behandeln, da offensichtlich ist, dass der Schaden, der durch eine Fehlleistung der Zertifizierungsdiensteanbieterin entstehen kann, die Wertgrenze der Nutzungsbeschränkung leicht überschreiten kann.

Es liegt auf der Hand, dass die Verfasser bei der Redaktion des VE dieselbe Absicht hegten. Wie eben skizziert, ist die in Art. 18 Abs. 3 gezeichnete Variante aber mehrdeutig. Wir beantragen deshalb eine Klarstellung der Bestimmung.

Swisskey Die im BGES vorgesehene Haftungsordnung erhöht das Haftungsrisiko des die elektronische Signatur Einsetzenden verglichen mit der heutigen Rechtlage. Die Haftung bzw. das Risiko sollte nach objektiven Kriterien - und nicht zum Zwecke des Konsumentenschutzes - verteilt werden.

Aus Sicht eines Zertifizierungsanbieters sind wir natürlich nicht glücklich über die im Gesetzesentwurf vorgeschlagene Haftungsregel zu unseren Lasten. Die Haftung geht zu weit. Ein Zertifizierungsanbieter kann sich nur durch den Nachweis der Erfüllung der Pflichten, die sich aus dem BGES ergeben, exkulpieren. Ansonsten haftet der Zertifizierungsanbieter vollumfänglich für jeden Schaden, welcher einem Inhaber eines privaten Signaturschlüssels oder einer Drittperson, entstehen. Grundsätzlich kann man im Haftpflichtrecht zwischen Verschuldens- und Kausalhaftung unterscheiden (nebst anderen rechtstheoretischen Unterscheidungskriterien). Die Schadenersatzpflicht bei der Verschuldenshaftung hat ihre Basis im Verschulden des Schädigers. Wesentlich dabei ist, dass für den Verursacher eines Schadens der Schadenseintritt voraussehbar war und er auch die entsprechenden Folgen erkennen kann. Ansonsten trägt er keine Verantwortung und es kommt der zentrale Grundsatz des Haftpflichtrechts zum Tragen: casum sentit dominus - der Geschädigte hat den Schaden selber zu tragen. In der Schweiz bildet die Verschuldenshaftung den allgemeinen Grundhaftungstatbestand, d.h. sofern das Gesetz nicht eine Kausalhaftung für einen Fall ausdrücklich vorsieht. Bei der Kausalhaftung wird eben auf das Element des Verschuldens und somit auf die Voraussehbarkeit verzichtet. Es werden vom Gesetz Personen als für einen Schaden verantwortlich bezeichnet, weiche den Schadenseintritt nicht konkret durch ihr Tun oder Unterlassen beeinflussen können bzw. die Möglichkeit der Schädigung nicht konkret voraussehen können. Bei der Verschuldenshaftung liegt ein tadelnswertes Verhalten des Schädigers - das Verschulden - vor; bei der Kausalhaftung ist dies aber gerade unabhängig vom Verhalten des Haftpflichtigen.

Des weiteren muss man sich vergegenwärtigen, dass die meisten Rechtsgeschäfte in der Schweiz formlos abgeschlossen werden können - nur wenige privatrechtliche Verträge erfordern eine bestimmte Form. Wenn sich die Haftung der Zertifizierungsanbieterin einzig und allein auf diejenigen Verträge beziehen würde, welche von Gesetzes wegen eine bestimmte Form erfordern und mit der elektronischen Unterschrift diese erfüllt wäre, so wäre die Haftung in bestimmten Grenzen abschätzbar. Da aber nun auch bei formlosen Geschäften eine elektronische Unterschrift eingesetzt wird, fallen auch diese gemäss dem BGES in den Risikobereich des Zertifizierdiensteanbieters. Eine solche Ausdehnung zu Lasten der Zertifizierdiensteanbieter ist nicht tragbar unter der Prämisse der Kausalhaftung. Eine Verschuldenshaftung demgegenüber würde

das Risiko insofern reduzieren, dass eine Zertifizierdiensteanbieterin danach strebt, keine Fehler zu begehen und ihre Aufgaben tadellos zu erfüllen.
Rechtsvergleichend ist darauf hinzuweisen, dass zum deutschen Signaturgesetz ein Entwurf zur Änderung vorliegt, welche von einer Verschuldenshaftung ausgeht (vgl. Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften; in der Fassung des Kabinettbeschlusses vom 16. August 2000). Im § 11 Absatz 2 SigG soll es neu wie folgt heissen: „Die Ersatzpflicht tritt nicht ein, wenn der Zertifizierungsdiensteanbieter nicht schuldhaft gehandelt hat“. Schon in der heute gültigen Version heisst es: „Die Ersatzpflicht des Zertifizierungsdiensteanbieters ist ausgeschlossen, wenn er die Verletzung nicht zu vertreten hat.“ Hinzuweisen ist in diesem Zusammenhang, dass im deutschen Recht die Schriftlichkeit weit häufiger gesetzlich verlangt ist und die elektronische Signatur eine höhere Bedeutung hat. Trotzdem geht der deutsche Gesetzgeber systemkonform von einer Verschuldenshaftung und nicht von einer Kausalhaftung aus.
Auch ist beim Einsatz verschiedener Komponenten (Kartenleser, Chipkarte, Browser) durch verschiedene Beteiligte (ISP, Telco, SW-Lieferant etc.) schwierig, die Verantwortung klar zuzuordnen.
Die im Begleitbericht aufgeführten Beispiele lassen ahnen, welche Schäden entstehen können. Ein solches von den Zertifizierungsanbietern zu tragende Risiko ist auch kaum versicherbar - zumindest nicht finanzierbar! Hier stellt sich ernsthaft die Frage, ob es in der Schweiz jemanden gibt, der ein solches Risiko tragen möchte - insbesondere, wenn der Markt nicht viel (am liebsten gar nichts) für ein Zertifikat bezahlen möchte. Es sollen hier nicht auf diese Weise konsumentenschutzpolitische Anliegen über die Kausalhaftung eingefügt werden. Wir fordern daher höchstens eine Verschuldenshaftung für Zertifizierungsanbieter.

321.19 Art. 19

Gerichte / Tribunaux / Tribunali

BGr Der Vollständigkeit halber erlauben wir uns in diesem Zusammenhang den Hinweis, dass Art. 19 des Bundesgesetzes über die elektronische Signatur die Ansprüche aus diesem Gesetz einer relativen einjährigen und einer absoluten zehnjährigen Verjährungsfrist unterstellt, welche Fristen als deliktische verstanden und an Art. 60 OR angelehnt werden (Begleitbericht S. 25 Ziff. 210.074). Nach der ebenfalls in Vernehmlassung befindlichen Vorlage zur Revision und Vereinheitlichung des Haftpflichtrechts sollen diese Fristen im Obligationenrecht auf drei bzw. zwanzig Jahre verlängert werden (Art. 55 E-OR). In dieser Frage besteht gegebenenfalls Harmonisierungsbedarf.

Kantone / Cantons / Cantoni

BS Im Begleitbericht sollte darauf hingewiesen werden, dass das neue Haftpflichtrecht andere Verjährungsfristen vorsieht, und dass die beiden Gesetze aufeinander abzustimmen sein werden.

LU Die Verjährungsfrist gemäss Art. 19 entspricht nicht den im Entwurf für ein Bundesgesetz über die Revision und Vereinheitlichung des Haftpflichtrechts vorgesehenen Fristen. Es sind keine Gründe ersichtlich, die für eine andere Regelung sprechen würden.

VD Le projet n'indique pas clairement pourquoi seule la prescription délictuelle d'une année a été retenue. En effet, dans l'hypothèse d'une action intentée par le titulaire du certificat contre le fournisseur de services de certification, le délai

de prescription devrait être celui de dix ans prévu par l'art. 127 du Code des obligations.

Organisationen / Organisations / Organizzazioni

Briner In Art.19 wird weder korrekt Art. 60 OR (und/oder Art. 127 ff. OR) zitiert, noch wird ersichtlich, ob oder in welcher Hinsicht ein Unterschied zu diesen Bestimmungen beabsichtigt ist.

Clusis L'art. 19 du prévoit une prescription annuelle à compter du jour où la partie lésée a eu connaissance du dommage et, dans tous les cas, pour dix ans dès le jour où le fait dommageable s'est produit, pour les *„actions prévues par la présente loi".* Or, force est de constater que la loi ne prévoit aucune action en tant que telle, sinon les dispositions pénales de l'art. 22, qui n'étaient certainement pas visées puisque l'art. 19, consacré à la prescription, fait partie de la section 7.

Dès lors, s'agit-il réellement de l'ensemble des actions découlant du projet de loi, qu'elles soient initiées ou dirigées contre le titulaire de la clé privée, le destinataire de messages signés, ou le fournisseur de services de certification ?

Il y a certainement là matière à clarification.

Jeune Barreau vaudois Wie / Comme / Come Clusis.

SBV Il y aurait lieu, le cas échéant, de compléter cette disposition en précisant, ainsi que le fait l'art. 60 CO, que l'action se prescrit un an à compter du jour où la partie lésée a eu connaissance du dommage ainsi que de la personne qui en est l'auteur. Cette dernière indication n'a pas été reprise à l'article 19 du projet de loi.

SWICO Ist hier auch die Kenntnis des Schädigers zu verlangen - analog zu OR Art. 60 -, um die relative Frist laufen zu lassen?

321.20 Art. 20

Kantone / Cantons / Cantoni

TI A nostro avviso devono essere precisate le condizioni per la trasmissione dei certificati elettronici quando le firme elettroniche sono gestite in altri paesi, rispettivamente quando il prestatore di servizi di certificazione opera dall'estero o disloca suo personale fuori dal territorio svizzero.

VD Il est inhabituel qu'une loi autorise le Conseil fédéral à conclure des conventions internationales.

Organisationen / Organisations / Organizzazioni

economiesuisse Die in Art. 20 vorgesehene Regelung der internationalen Anerkennung von elektronischen Signaturen vermag nicht zu befriedigen, denn das Problem der gegenseitigen Anerkennung lässt sich wohl nicht fristgerecht allein mittels bilateraler bzw. multilateraler Verträge lösen, was dem grenzüberschreitenden E-Commerce kaum förderlich ist. Daher ist, in Anlehnung an Art. 7 Abs. 1 lit. b der EG-Richtlinie, folgendes aufzunehmen:

„Die Schweiz anerkennt elektronische Zertifikate, die von einem in einem Drittland anerkannten Anbieter von Zertifizierungsdiensten ausgestellt werden, vorausgesetzt, dass ein unter dem BGES anerkannter Anbieter von Zertifizierungsdiensten für das Zertifikat dieses ausländischen Anbieters von Zertifizierungsdiensten einsteht."

Diese Alternative ist deshalb sachgerecht, weil dann nicht der Staat, sondern der Markt darüber entscheidet, ob ein ausländisches einem schweizerischen Zertifikat gleichgestellt ist. Denn ein schweizerischer Anbieter würde nur für ein

ausländisches Zertifikat, das einem schweizerischen gleichwertig ist, die Haftung übernehmen wollen.

FHZ Eine schnelle Umsetzung dieser Zielsetzungen muss garantiert werden. Eine gegenseitige Anerkennung ist ein Hauptangelpunkt dafür, ob sich die digitale Signatur im nationalen sowie internationalen Bereich durchsetzen kann.

SAV Le projet donne la compétence au Conseil fédéral de conclure des conventions internationales sur la reconnaissance des signatures électroniques, mais il ne dit rien sur la reconnaissance de ces signatures en droit interne, malgré le titre de la loi. C'est dans le code des obligations et dans d'innombrables lois qu'il faut rechercher la possibilité d'utiliser des signatures électroniques.

SWICO Hier muss eine klare Regel aufgestellt werden, wann ausländische Signatursysteme anerkannt werden. Eine Globalverweisung genügt auf keinen Fall. Zumindest die in der EU zugelassenen Systeme, welche gemäss Richtlinie und nationaler Gesetzgebung akkreditiert wurden, müssten automatisch auch Anerkennung in der Schweiz finden. Dies gilt sowohl für Zertifizierungssysteme wie auch zugelassene Komponenten.

SwissICT Vgl. zu Art. 4 / Cf. ad art. 4 / Cfr. ad art. 4.

321.21 Art. 21

Kantone / Cantons / Cantoni

BS Vgl. zu Art. 5 / Cf. ad art. 5 / Cfr. ad art. 5.

GE Selon le rapport explicatif, l'attestation de la conformité d'une signature numérique prévue par l'art. 21 ne serait pas une décision administrative sujette à recours, mais le simple constat d'un fait. Cela peut se comprendre dans la perspective d'une libre appréciation des preuves par le juge, d'une part, et du risque qu'une décision non attaquée en temps utile n'acquière un caractère définitif et exécutoire, d'autre part. Toutefois, il ne faut pas s'imaginer qu'un juge pourrait aisément se distancer du constat qu'établirait l'organisme d'accréditation et, surtout, il ne faudrait pas que le caractère non décisionnaire d'un tel constat prive les intéressés de la possibilité de participer à ce qui apparaît quand même comme une procédure tendant à l'obtention d'un tel constat. De plus, la qualification juridique donnée au constat en question ne résulte pas de l'avant-projet de loi, mais uniquement du rapport explicatif qui l'accompagne.

TG Der in Art. 21 geregelten Bestätigung der Konformität einer digitalen Signatur durch die Akkreditierungsstelle dürfte vorab in Rechtsöffnungsverfahren grosse Bedeutung zukommen. Entgegen dem Wortlaut von Art. 21 sollte allerdings die Akkreditierungsstelle nicht nur zur Ausstellung einer Bestätigung der digitalen Signatur und der Gültigkeit derselben verpflichtet werden; vielmehr müsste die Stelle auch den Inhalt des elektronischen Dokuments auf Papier festhalten. Die elektronischen Dokumente müssen in eine lesbare Form gebracht werden, da die Gerichte nicht über sämtliche auf dem Markt erhältlichen Programme verfügen können, insbesondere nicht in der jeweils neuesten Version; andernfalls wären die Gerichte selbst nicht immer in der Lage, entsprechende elektronische Dokumente zu lesen.

VD L'on peut se demander quelle est la responsabilité d'un organisme d'accréditation concernant l'attestation écrite de l'alinéa 1 de cette disposition.

VS L'émolument prévu à l'art. 21 devra réellement rester modeste, sans quoi il dissuadera rapidement une grande partie de la population d'utiliser la voie électronique, eu égard au renversement du fardeau de la preuve posé à l'art. 17 et au renvoi des litiges entre fournisseurs et organismes de reconnaissance au for civil (rapport p. 16).

Organisationen / Organisations / Organizzazioni

Briner Der Begleitbericht erwähnt, dass die ZertD-Anbieterinnen privatrechtlich tätig werden und dass die Zertifikate privatrechtlich ausgestellt werden. In welcher Eigenschaft (öffentlich- oder privatrechtlich) wird aber die Akkreditierungsstelle gemäss Art. 21 tätig? Man hat den Eindruck, es sei eine öffentlichrechtliche Tätigkeit. Was aber, wenn die Akkreditierungsstelle (aus welchen Gründen auch immer) eine sachlich unrichtige Bestätigung abgibt? Ist der Gegenbeweis zur Bestätigung möglich, obwohl der Staat hoheitlich handelt? Da die Zertifikate eine privatrechtliche Sache sind, sähe sich der Staat in der eigenartigen Position, hoheitliche Bestätigungen über privatrechtliche Verhältnisse abzugeben. Uns scheint, diese Problematik sollte vertieft geprüft und genauer geregelt werden.

economiesuisse Dieser Artikel, bzw. der ganze 9. Abschnitt, ist ersatzlos zu streichen. Grundsätzlich ist davon auszugehen, dass die in Anwendung dieses Gesetzes verwendeten und durch entsprechende Zertifikate bescheinigten digitalen Signaturen gesetzeskonform sind. Es ist daher nicht einzusehen, weshalb das Gesetz für diese Erkenntnis eine weitere, gebührenpflichtige Bestätigung vorschreibt.

Auch die im Begleitbericht angegebene fehlende Infrastruktur und das mangelhafte Fachwissen seitens der Gerichte vermögen als Begründung nicht zu überzeugen. Dazu kommt, dass diese im Gesetz vorgesehene Möglichkeit einer Bestätigung wohl über kurz oder lang zum Standard wird, was einen unnötigen administrativen und finanziellen Zusatzaufwand zur Folge hat. Ein gültiges Zertifikat vermag diese Kontrollfunktion durchaus zu erfüllen, weitere Instrumente sind dazu nicht nötig. Schliesslich ist anzufügen, dass mit dem Erfordernis des Zeitstempels sämtliche Unsicherheiten bezüglich Gültigkeit des Zertifikats in einem bestimmten Zeitpunkt ausgeräumt sind.

Muster/Sury Der Aufwand der Verifikation einer Signatur kann unter Umständen beträchtlich sein, insbesondere wenn für Ablage und den Anhang des Zertifikats ein proprietäres Format verwendet worden ist. Zudem kann die Verifikation Schwierigkeiten bereiten, wenn das entsprechende Dokument zuerst signiert, dann verschlüsselt worden ist. Eine fixe Gebühr kann unter Umständen in keinem Verhältnis zum anstehenden Aufwand sein.

SBV L'art. 21 de loi prévoit que l'organisme d'accréditation atteste, sur demande, qu'un certificat électronique „était valable à un moment donné“. Cette disposition ne fait que souligner la nécessité de disposer d'un service d'horodatation („time stamping“), ainsi que nous l'avons demandé dans notre commentaire relatif à l'art. 3. Nous proposons dès lors, pour le cas où un service d'horodatation serait introduit, de supprimer cette disposition.

SWICO Im selben Sinne wie / Dans le même sens que / Nello stesso senso che economiesuisse.

TSM Art. 21 erklärt, dass die Akkreditierungsstelle gegen eine Gebühr die auf einem elektronischen Dokument vorhandene digitale Signatur bestätigt. Hierbei ist uns wichtig, dass diese Gebühr nach dem Verursacherprinzip erhoben wird.

321.22 Art. 22

Kantone / Cantons / Cantoni

BE Gemessen am Schaden, der entstehen kann, erachten wir die Höchstbusse von 100'000 Franken als zu tief und schlagen einen Höchstbetrag von 500'000 Franken vor.

BS Für die Strafbestimmung von Art. 22 Abs. 1 schlagen wir folgende Textergänzung vor:
„[1]Wer als Anbieterin von Zertifizierungsdiensten vorgibt, über die Anerkennung nach diesem Gesetz zu verfügen, oder wer Zertifikate nach diesem Gesetz ausstellt, ohne die Angaben nach Artikel 8 *vollständig und wahrheitsgemäss* zu machen, wird auf Antrag mit Busse bis zu 100'000 Franken bestraft."
Wegen der starken Ähnlichkeit der geschützten Rechtsgüter könnte die unseres Erachtens unzutreffende Auffassung vertreten werden, Art. 22 BGES sei gegenüber Art. 251 StGB lex specialis. Hier wäre eine entsprechende Klarstellung in Art. 22 angebracht, zum Beispiel durch die Formulierung (in Abs. 1): „[1]Wer als Anbieterin von Zertifizierungsdiensten vorgibt, über die Anerkennung nach diesem Gesetz zu verfügen, oder wer Zertifikate nach diesem Gesetz ausstellt, ohne die Angaben nach Artikel 8 vollständig und wahrheitsgemäss zu machen, wird**,** *sofern nicht ein Tatbestand gemäss Strafgesetzbuch erfüllt ist,* auf Antrag mit Busse bis zu 100'000 Franken bestraft."
Aus der Sicht der Strafverfolgungsbehörden wäre ein Hinweis auf den massgeblichen Gerichtsstand in Abs. 4 von Art. 22 sehr erwünscht, weil ein Delikt dieser Art doch regelmässig verschiedene Anknüpfungspunkte aufweisen dürfte und deshalb negative Kompetenzkonflikte unter den Kantonen vorauszusehen sind.

GL Nach Art. 22 Abs. 1 wird auf Antrag mit Busse bis zu Fr. 100'000 bestraft, wer als Anbieterin von Zertifizierungsdiensten vorgibt, über die Anerkennung nach dem Gesetzesentwurf zu verfügen, oder wer Zertifikate nach diesem Gesetz ausstellt, ohne die Angaben gemäss Art. 8 zu machen. Nicht ganz einzusehen ist, warum die Verletzung von anderen im Gesetzesentwurf vorgesehenen wesentlichen Pflichten durch anerkannte Anbieterinnen von Zertifizierungsdiensten nicht unter Strafe gestellt werden soll. Es wird daher angeregt, die Aufzählung in Art. 22 Abs. 1 mit den entsprechenden Tatbeständen, allenfalls mit einer Generalklausel, zu ergänzen. Weiter kommt die Stellung der anerkannten Anbieterinnen von Zertifizierungsdiensten insbesondere in Bezug auf die Gewährleistung der Authentizität von übermittelten Informationen jener einer Urkundsperson nahe. Unter Berücksichtigung der erhöhten Vertrauensstellung der anerkannten Anbieterinnen von Zertifizierungsdiensten erscheint damit die Ausgestaltung von Art. 22 als Vergehenstatbestand gerechtfertigt. Die anerkannten Anbieterinnen von Zertifizierungsdiensten zeichnen sich - etwa im Unterschied zu den in Art. 23 UWG erfassten durchschnittlichen Marktteilnehmern - durch eine ausgeprägte Vertrauensstellung aus. Die Verletzung dieser Vertrauensstellung würde daher rechtfertigen, Art. 22 BGES statt als Antrags- als Offizialdelikt auszugestalten.

JU Il convient de relever ici que tel que rédigé, l'al. 1 rend punissable celui qui prétend être un fournisseur de services de certification reconnu au sens de la loi, quand bien même il serait effectivement au bénéfice d'une reconnaissance en bonne et due forme. Au regard du commentaire figurant dans le rapport explicatif, cela résulte toutefois vraisemblablement d'une inadvertance.

SO Mit Art. 22 wird lediglich das ungesetzliche Anbieten von elektronischen Signaturen auf Antrag unter Strafe gestellt. Das Legalitätsprinzip (Art. 1 StGB) und die Rechtssicherheit würden hier eine Strafnorm verlangen, die derjenigen gegen Urkundenfälschung (Art. 251 StGB) entsprechen würde. Da die Verbreitung der elektronischen Signatur und die Häufigkeit deren Missbrauchs heute noch nicht abschätzbar sind, erachten wir den Erlass einer speziellen Strafnorm im Range eines Offizialdelikts als nicht dringlich.

VD Cette disposition ne prévoit qu'une simple contravention poursuivie sur plainte. Compte tenu des conséquences graves que peuvent avoir certaines violations des règles contenues dans la loi et du très bref délai de prescription pour les contraventions, cette réglementation paraît insuffisante.
Face aux intérêts importants en jeu, il paraît opportun de prévoir, selon une technique législative courante, que les autres infractions aux dispositions de la loi et de ses ordonnances d'exécution constituent une contravention.
Enfin, le terme „etc.“ mentionné à l'al. 3 n'a pas sa place dans une loi, à plus forte raison dans ses dispositions pénales.

ZH Nach Art. 22 Abs. 1 wird auf Antrag mit Busse bis zu Fr. 100’000 bestraft, wer als Anbieterin von Zertifizierungsdiensten vorgibt, über die Anerkennung nach dem Gesetzesentwurf zu verfügen, oder wer Zertifikate nach diesem Gesetz ausstellt, ohne die Angaben gemäss Art. 8 zu machen. Nicht ganz einzusehen ist, warum die Verletzung von anderen im Gesetzesentwurf vorgesehenen wesentlichen Pflichten durch anerkannte Anbieterinnen von Zertifizierungsdiensten nicht unter Strafe gestellt werden soll. So könnten etwa vorsätzlich falsch gemachte Angaben im Tätigkeitsjournal (Art. 10 Abs. 3) die Wahrnehmung wichtiger aufsichtsrechtlicher Pflichten stören oder vereiteln, falsche Angaben im Verzeichnis für ungültig erklärte oder suspendierte Zertifikate (Art. 12 Abs. 2) oder die Unterlassung einer Ungültigerklärung elektronischer Zertifikate (Art. 11 Abs. 1) zu grossen wirtschaftlichen Schäden führen. Dem Begleitbericht sind keine Angaben über die Gründe für den eng umschriebenen Tatbestand in Art. 22 Abs. 1 zu entnehmen. Es wird daher angeregt, die Aufzählung in Art. 22 Abs. 1 mit den entsprechenden Tatbeständen, allenfalls mit einer Generalklausel, zu ergänzen.
Der Vergleich zwischen Art. 22 BGES und Art. 23 UWG lässt vermuten, dass Letzterer die Vorlage zur Ausgestaltung der Strafbestimmung im vorliegenden Gesetzesentwurf lieferte. Angesichts der entscheidenden Funktion, die den anerkannten Anbieterinnen von Zertifizierungsdiensten für die Sicherheit im Umgang mit der digitalen Signatur zukommt, ist indes nicht ganz nachvollziehbar, warum Art. 22 BGES lediglich als Übertretungstatbestand konzipiert ist. Die Stellung der anerkannten Anbieterinnen von Zertifizierungsdiensten kann insbesondere in Bezug auf die Gewährleistung der Authentizität von übermittelten Informationen jener einer Urkundsperson nahe kommen. Unter Berücksichtigung der erhöhten Vertrauensstellung der anerkannten Anbieterinnen von Zertifizierungsdiensten erscheint damit die Ausgestaltung von Art. 22 als Vergehenstatbestand (... Gefängnis oder Busse bis zu Fr. 1000 000...) gerechtfertigt.
In der Regel werden Straftatbestände dann als Antragsdelikte ausgestaltet, wenn eine Straftat einen geringen Unrechtsgehalt aufweist, das Strafverfahren die Persönlichkeitssphäre der oder des Verletzten regelmässig stark berührt oder wenn die Strafverfolgung enge persönliche Beziehungen zwischen Opfer und Täter beeinträchtigen könnte. Keines der dargelegten Kriterien ist vorliegend erfüllt. Die anerkannten Anbieterinnen von Zertifizierungsdiensten zeichnen sich hingegen - etwa im Unterschied zu den in Art. 23 UWG erfassten durchschnittlichen Marktteilnehmern - wie bereits erwähnt durch eine ausgeprägte Vertrauensstellung aus. Die Verletzung dieser Vertrauensstellung würde daher rechtfertigen, Art. 22 statt als Antrags- als Offizialdelikt auszugestalten.
Konsequenterweise müsste mit der Konzeption von Art. 22 als Vergehenstatbestand Art. 19 nach Vorbild von Art. 60 Abs. 2 OR um einen zweiten Absatz erweitert werden («Werden jedoch Ansprüche aus einer strafbaren Handlung

hergeleitet, für die das Strafrecht eine längere Verjährung vorschreibt, gilt diese auch für den Zivilanspruch»).

Organisationen / Organisations / Organizzazioni

Briner Wir erachten es als sehr unzweckmässig, in Art. 22 Abs. 2 für die Aktivlegitimation auf UWG zu verweisen, weil damit impliziert wird (oder werden könnte?), dass die Aktivlegitimation selber ein Wettbewerbsverhältnis im Sinne des UWG erfordert.

economiesuisse Diese Bestimmung nennt zwei Fälle. Auch im zweiten Fall handelt es sich beim Täter um eine Anbieterin von Zertifizierungsdiensten; Tatbestand ist dabei, dass sie es unterlassen hat, in den ausgestellten Zertifikaten alle Angaben gemäss Art. 8 aufzunehmen. Dass es sich dabei um eine anerkannte Anbieterin handeln muss, ist im Gesetz aber ausdrücklich festzuhalten, sind doch auch nicht anerkannte Anbieter zulässig, deren Handlungen jedoch nicht vom vorliegenden Gesetz erfasst werden. Entsprechend wäre Abs. 1 wie folgt zu ergänzen: „..., oder wer als *anerkannte* Anbieterin Zertifikate nach diesem Gesetz ausstellt, ...".

FGSec Zu Abs. 1: Die EU-Direktive erlaubt die Ausstellung qualifizierter Zertifikate auch ohne Akkreditierung. Es ist klar aus dem Begleitbericht, dass dies in der Schweiz nicht erlaubt sein wird. Dies geht aber nicht aus dem BGES-Text hervor. Ist dies EU-kompatibel? Was liegt in unserem Interesse?

ISACA „….prévus à l'article 9 …".

SBV Il devrait être fait mention, dans la loi, que seuls les prestataires de services de certification reconnus sont, dans ce cas, passibles d'une amende. Nous proposons de préciser cette disposition dans le sens indiqué.

SWICO Diese Bestimmung nennt zwei Fälle: (i)Täter ist eine nicht anerkannte Zertifizierungsstelle, die vorgibt, sie sei eine anerkannte; (ii)Täter ist eine anerkannte Zertifizierungsstelle, die aber in den ausgestellten Zertifikaten nicht alle Angaben gemäss Art. 8 aufnimmt. Für den Fall (ii) muss somit im Gesetz der Täter noch umschrieben werden, d.h. dass es sich eben um eine anerkannte Zertifizierungsstelle handelt, denn auch nicht-anerkannte Zertifizierungsstellen sind zulässig, deren Geschäftstätigkeit jedoch vom BGES nicht geregelt ist.

321.23 Art. 23

Kantone / Cantons / Cantoni

SG Wir beantragen, Art. 23 Abs. 1 Satz 3 an geeigneter Stelle im 5. Abschnitt zu integrieren.

Begründung: Aufbewahrung und Zugriffssicherung der elektronischen Zertifikate sind zentrale Aufgaben der Anbieterinnen von Zertifizierungsdiensten. Die Festschreibung einer entsprechenden Pflicht in den materiellen Bestimmungen des Gesetzes erscheint zwingend.

Wir beantragen, in den Ausführungsvorschriften der allfälligen Notwendigkeit zur Anpassung der technischen Komponenten der elektronischen Signatur Rechnung zu tragen.

Begründung: Wenn für elektronische Signaturen eingesetzte Algorithmen und Parameter - und dadurch die damit erzeugten elektronischen Signaturen - infolge des technischen Fortschritts an Sicherheitswert verlieren, ist eine rechtzeitige Anpassung der technischen Komponenten erforderlich. Um zu verhindern, dass neue elektronische Signaturen zu einem späteren Zeitpunkt angebracht und zurückdatiert werden, ist für diese überdies ein Zeitstempel erforderlich. Damit frühere elektronische Signaturen im Hinblick auf eventuelle

spätere Fälschungsmöglichkeiten nicht bestritten werden können, müssen diese in die neue Signatur eingeschlossen und damit „konserviert“ werden.

VD L'al. 2 pourrait avoir des conséquences sur l'infrastructure technique des cantons et engendrer des coûts non négligeables. Il conviendrait dès lors de prévoir une consultation des cantons avant l'adoption de ces prescriptions.

Parteien / Partis / Partiti

PLS Il nous paraît essentiel que, dans le cadre de la rédaction des clauses d’exécution, le Conseil fédéral consulte systématiquement les milieux économiques intéressés. En effet, il est important que l’économie puisse intervenir dans ce contexte car, en définitive, elle exercera une influence déterminante sur l’utilisation dans les échanges commerciaux des certificats électroniques.

Organisationen / Organisations / Organizzazioni

economiesuisse Mit der Kompetenzdelegation an den Bundesrat, die (sicherheits)technischen und verfahrensmässigen Details in den Ausführungsbestimmungen zu regeln, wird zwar ein System geschaffen, das der technischen Entwicklung und der damit erforderlichen Flexibilität bei gesetzgeberischen Anpassungen Rechnung trägt. Andererseits fehlen unseres Erachtens die Mindestanforderungen an die digitale Signatur und an das (qualifizierte) Zertifikat in technischer wie qualitativer Hinsicht; diese sollten aber auf Gesetzesebene abgebildet werden. Diese Anregung steht somit im Spannungsfeld zwischen Flexibilität der Regelung und Rechtssicherheit. Entsprechend muss bei der Formulierung solcher Mindestanforderungen beachtet werden, dass zwar der Spezifikationsgrad zu Gunsten der Rechtssicherheit erhöht wird, ohne sich (zu sehr) hinsichtlich der Regelungsmöglichkeiten auf Verordnungsebene einzuengen. Im Gesetzesentwurf sind somit gewisse Mindestanforderungen - vergleichbar zur EU-Richtlinie - an die digitale Signatur bzw. an Kryptographie und privaten Signaturschlüssel sowie an das Zertifikat, sowohl in technischer wie auch in qualitativer Hinsicht, aufzunehmen.

Wir halten fest, dass die Kompetenz des Bundesrates für den Erlass von Ausführungsbestimmungen inklusive einer möglichen Subdelegation sehr weit geht. Diese Gesetzestechnik lässt sich durch die technische Natur der Vorlage begründen. Wir wünschen jedoch, dass die betroffenen Kreise und die Wirtschaftsorganisationen zu den kommenden Ausführungsbestimmungen konsultiert werden.

Schlauri/Kohlas Art. 23 Abs. 1 delegiert u. a. die Festlegung der Dauer der Aufbewahrungspflicht für Certificate Revocation Lists (CRL) an den Bundesrat. In Art. 13 ZertDV ist derzeit eine Aufbewahrungspflicht von elf Jahren vorgesehen. Diese Aufbewahrungspflicht sollte u.E. auf eine bedeutend längere Zeitdauer als elf Jahre ausgedehnt werden.

Denn der wohl hinter der Beschränkung stehende Gedanke, dass nach zehn Jahren die Verjährung abgelaufen ist und damit keine Notwendigkeit für eine weitere Aufbewahrung notwendig ist, greift bei Dauerschuldverhältnissen allenfalls zu kurz.

Der durch eine solche Verlängerung der Aufbewahrungszeit geschaffene zusätzliche Aufwand für die Zertifizierungsdiensteanbieter hält sich – anders als es auf den ersten Blick scheinen mag – in engen Grenzen: Bei der hie und da sowieso notwendigen Formatkonvertierung der Zertifikatsdatenbanken (etwa bei Verabschiedung neuer Standards) wird immer ein Teil der Datensätze in das Zielformat übertragen werden müssen, weil deren Aufbewahrungsfrist noch nicht abgelaufen ist. Und ob nun eine komplette Datenbank oder nur die in den

vergangenen 11 Jahren aufgelaufenen Daten konvertiert werden müssen, beeinflusst die Kosten nur unwesentlich.
Der im Laufe der Zeit durch die Weiterentwicklung der Technik entstehenden Verwundbarkeit der Signierschlüssel kann im Übrigen durch periodisches Versehen des signierten Dokumentes mit einem neuen Zeitstempel vorgebeugt werden: Wenn der neue Zeitstempel immer vor dem Verfall des alten Zertifikates bzw. des vorhergehenden Zeitstempels gesetzt wird, entsteht eine nicht zu brechende Beweiskette, welche das alte Zertifikat den Zeitablauf beliebig überdauern lässt.

SBV Le projet de loi se caractérise par des délégations de compétences très étendues en faveur du Conseil fédéral. Si de tels renvois peuvent paraître justifiés au regard de l'évolution très rapide de la technologie, il n'en demeure pas moins difficile, dans ces conditions, de mesurer la portée exacte de la loi. Nous estimons dès lors que les milieux de l'économie doivent être étroitement associés à l'élaboration des dispositions d'exécution de la loi. Cela d'autant plus que celles-ci auront, en définitive, une influence déterminante sur l'utilisation, dans les échanges commerciaux, de certificats électroniques délivrés conformément à la loi.
Afin de faciliter la consultation de la loi, nous proposons par ailleurs de faire référence, à l'art. 23, à toutes les dispositions donnant compétence au Conseil fédéral de compléter la loi, dans le cadre des dispositions d'exécution. Cette solution est celle retenue par la loi allemande révisée sur la signature électronique (cf. § 24 de cette loi).

SWICO Hier sollten u.E. alle Gesetzesbestimmungen aufgeführt werden, die dem BR die Kompetenz einräumen, Näheres (bzw. Ergänzendes) zum BGES zu regeln, soweit dies im Rahmen dieser technischen Ausführungsbestimmungen erfolgen soll. Es dürften alle Kompetenzdelegationen betreffen mit Ausnahme von Art. 2 Abs. 2 und Art. 20.

321.24 Art. 24

Kantone / Cantons / Cantoni

BS Der Kommentar in Ziff. 210.112 des Begleitberichtes erweckt den Eindruck, die Zertifizierungsdiensteverordnung falle von alleine dahin.

322 Änderungen von Bundesgesetzen
Modifications de lois fédérales
Modifica di leggi federali

322.1 Im Allgemeinen / En général / In generale

Kantone / Cantons / Cantoni

AI Unklar ist, ob im Geschäftsverkehr mit der öffentlichen Hand eine solche PKI verwendet werden sollte. Hier besteht seit Jahren dringender Handlungsbedarf, hängt doch ein enormes Planungsvolumen an dieser unbeantworteten Frage.
Es wäre absolut möglich und wünschbar, wenn bei diesbezüglichen Überlegungen die Randregionen, zu denen sich der Kanton Appenzell I.Rh. zählt, berücksichtigt werden könnten (Entgegenwirken des Zentralismus).

BE Gemäss dem neuen Art. 949a Abs. 2 lit. e ZGB ist der Bundesrat betreffend die Führung des Grundbuchs mit EDV gehalten, Regelungen zur langfristigen Sicherung von Daten zu erlassen. In den entsprechenden, revidierten Bestimmungen des OR, Topografie-, Markenschutz- wie auch des Patentgesetzes

scheint uns eine Ergänzung in Bezug auf die Datensicherung bei der Registerführung gleichermassen angebracht. Bei einem zunehmend elektronischen Datenverkehr muss die Informationssicherung jederzeit gewährleistet werden können. Entsprechende Bestimmungen sollten - wenn nicht ins Gesetz selbst - in eine entsprechende Vollzugsverordnung aufgenommen werden. Die Archivierung elektronischer Daten scheint uns ebenfalls ein nicht thematisiertes Problem.

BS Der Erlass eines Gesetzes über die elektronische Signatur ist notwendig. Der Bereich der Grundbuchanmeldungen und Belege sollte dagegen im Interesse der Rechtssicherheit und der Gewährleistung der Eigentumsgarantie ausdrücklich von der Anwendung ausgeschlossen werden.

Viele elektronisch abgeschlossenen Geschäfte sind nach relativ kurzer Zeit erledigt und vollzogen; die elektronischen Geschäftsunterlagen werden dann nicht mehr benötigt. Die Pflicht zur Aufbewahrung der Geschäftsbücher endet gemäss Art. 962 Abs. 1 OR nach zehn Jahren. Die in das Grundbuch aufgenommenen Rechte und Pflichten hingegen sind auf Dauer angelegt und die Grundbuchbelege müssen noch nach Jahrzehnten als Beweismittel dienen können. Der Bereich der Grundbuchanmeldungen und Belege sollte darum für die elektronische Signatur erst dann zugänglich gemacht werden, wenn sich die dafür erforderlichen technischen Einrichtungen langfristig bewährt haben und Gewissheit darüber besteht, dass sie auch noch nach Jahrzehnten ihren Zweck erfüllen, gelesen werden und als Beweismittel dienen können.

Es ist sinnvoller, wenn die neuen Technologien schrittweise eingeführt werden und zunächst in anderen Bereichen Erfahrungen gesammelt werden. Auch besteht bei den Grundbuchanmeldungen und den Belegen im Augenblick kein Bedürfnis, die elektronische Signatur anzuerkennen, spielt doch das Zeitelement im Geschäftsverkehr mit dem Grundbuch aufgrund von Art. 972 ZGB („Die Wirkung einer Eintragung wird auf den Zeitpunkt der Einschreibung in das Tagebuch zurückbezogen“) keine derart ausschlaggebende Rolle wie z.B. im Bankenverkehr oder auch im Prozessrecht.

Die im Gesetzesentwurf vorgesehene Möglichkeit, künftig mit dem Handelsregisteramt elektronisch zu kommunizieren, entspricht einem Anliegen nicht nur der Handelsregisterämter, sondern auch derjenigen Kreise der Wirtschaft, welche zu den Hauptkundinnen und Hauptkunden der Handelsregisterämter gehören. Von Seiten der Wirtschaft wird in den vergangenen Jahren immer mehr das Bedürfnis nach einer rascheren Erbringung der Dienstleistungen des Handelsregisters laut. So beträgt beispielsweise beim Handelsregisteramt des Kantons Basel-Stadt der Zeitraum zwischen dem Eingang eines Geschäftes und dessen Eintragung ins Handelsregister lediglich ein bis zwei Arbeitstage; dies sofern die eingereichten Belege den gesetzlichen Anforderungen entsprechen. Damit ist die Dauer des Eintragungsverfahrens im Vergleich zur übrigen Schweiz sehr kurz. Gleichwohl wird insbesondere im Verfahren, wo Belege zu korrigieren oder zu ergänzen sind, ein noch rascherer Datenaustausch und eine noch raschere Abwicklung des Korrekturverfahrens gefordert. Vielfach erscheint selbst die durch den Postversand der zu korrigierenden Belege verstreichende Zeit für die Kundinnen und Kunden des Handelsregisteramtes nicht akzeptabel, sodass sie zur Vornahme der erforderlichen Korrekturen direkt beim Handelsregisteramt vorsprechen.

Der elektronische Austausch von Daten würde die Dauer des Eintragungsverfahrens weiter verkürzen und insofern den Bedürfnissen der Wirtschaft Rechnung tragen. Immerhin sei in diesem Zusammenhang angemerkt, dass

selbst bei elektronischem Datenaustausch die Belege noch immer gelesen und kontrolliert werden müssen. Insofern sind der Reduktion des Zeitraumes zwischen Eingang und Eintragung eines Geschäftes Grenzen gesetzt.
Die elektronische Kommunikation mit den Handelsregisterämtern setzt voraus, dass diese Form der Kommunikation standardisiert und vor allem detailliert vorbereitet werden muss. Selbst die Form der Archivführung, welche seit der Einführung des Handelsregisters in der heute gängigen Form im Jahre 1883 auf Papier erfolgt, ist neu zu überdenken. Dabei gilt es insbesondere zu berücksichtigen, dass selbstverständlich mit der Einführung der elektronischen Kommunikation mit den Handelsregisterämtern der bisher übliche Papierweg nicht ersatzlos wegfällt. Vielmehr müssen beide Formen der Einreichung von Handelsregisterbelegen möglich sein und bleiben. Gerade diese parallele Führung eines elektronischen und eines Papierarchives wirft zahlreiche Fragen auf, die im Moment noch nicht gelöst sind. Erst wenn diese und zahlreiche weitere Fragen einer tragbaren und dauerhaften Lösung zugeführt sind, wird die elektronische Einreichung von Handelsregisterbelegen (Anmeldungen, Protokolle etc.) möglich sein.
Ein zusätzliches Problem stellt sich im gegebenen Zusammenhang bei der Gestaltung und Einreichung von öffentlichen Urkunden. Hier gilt es zu beachten, dass am Erfordernis der öffentlichen Beurkundung im Bereich des Gesellschaftsrechts da, wo sie heute vorgesehen ist, festzuhalten ist. Gleichzeitig gilt es zu berücksichtigen, dass sich selbst bei der Einführung der Verwendung von elektronischen Signaturen im Bereich des Notariats am Ablauf der Durchführung einer öffentlichen Beurkundung grundsätzlich nichts ändert. Die Form der öffentlichen Beurkundung bleibt infolgedessen praktisch unangetastet. So ist beispielsweise daran festzuhalten, dass die Parteien oder ihre Vertreterinnen oder Vertreter persönlich bei der verurkundenden Notarin oder beim verurkundenden Notar erscheinen müssen. Die Verwendung von elektronischen Signaturen auch in diesem Bereich hat lediglich Einfluss darauf, in welcher Form die Belege physisch vorhanden sind und den Handelsregisterämtern eingereicht werden. Da es jedenfalls im Moment eher unwahrscheinlich erscheint, dass die bei der Notarin oder beim Notar vorsprechenden Parteien den Inhalt der Urkunden via Bildschirm zur Kenntnis nehmen werden, werden die Belege im notariellen Bereich - jedenfalls nach derzeitigem Stand der Technik - noch lange in Papierform vorhanden sein. Es muss der Notarin oder dem Notar aber offenstehen, die Belege einzulesen, d. h. zu scannen, und in der Folge dem Handelsregisteramt elektronisch einzureichen. Es handelt sich in diesem Falle um eine besondere Form der beglaubigten Abschrift einer Urkunde, welche im Rahmen einer erforderlichen Neugestaltung des kantonalen Notariatsrechts zuzulassen wäre.

LU Zusammen mit dem BGES werden die Grundlagen geschaffen, dass beispielsweise Anmeldungen beim Grundbuchamt oder beim Handelsregisteramt auf elektronischem Weg erfolgen können. Hierfür sind noch Ausführungsbestimmungen des Bundesrates nötig. Beim Entscheid über die Inkraftsetzung dieser neuen Form des Geschäftsverkehrs ist den Kantonen genügend Zeit einzuräumen, damit die für die Realisierung notwendigen organisatorischen und technischen Änderungen vorgenommen werden können.

GR Die Vorlage schafft die gesetzliche Grundlage dafür, dass in Zukunft mit dem Handelsregister, dem Grundbuch und den im Immaterialgüterrecht vorgesehenen Registern elektronisch kommuniziert werden kann. Die Regierung begrüsst die Bestrebungen des Bundes zum Ausbau des elektronischen Behör-

denverkehrs. Der Kanton Graubünden wirkt denn auch beim Projekt „Guichet virtuel“ aktiv mit. Die grundsätzliche Unterstützung dieses Vorhabens entbindet jedoch nicht davon, für die verschiedenen Bereiche genau zu prüfen, welches die allfälligen Auswirkungen im Vollzug, namentlich für die Kantone, sein werden. Auch ist bei der Umsetzung dem unterschiedlichen Entwicklungsstand der verschiedenen Einrichtungen Rechnung zu tragen. Insbesondere sind aber auch die finanziellen Konsequenzen im Auge zu behalten. Aus kantonaler Sicht erscheint es daher gerechtfertigt, dass der Bund sich in einem gewissen Masse an den anfallenden Kosten beteiligt.

SG Im Bereich des elektronischen Verkehrs mit den Behörden (E-Government) bringt das neue Gesetz unmittelbar – ausser dem Verkehr mit bestimmten Registern – nur bescheidene Fortschritte. Um die breite Akzeptanz und die schnelle Verbreitung der elektronischen Signatur zu fördern, muss der Staat deren Einsatz auch in seinen Kundenbeziehungen zulassen. Für die Bürgerinnen und Bürger wäre es kaum nachvollziehbar, wenn ihre elektronische Signatur im Bereich des Privatrechts anerkannt wäre, im Behördenverkehr hingegen nicht. Daraus ergibt sich für Bund und Kantone die Notwendigkeit, je zu ihrem Zuständigkeitsbereich möglichst bald auch die Rechtsgrundlagen für rechtsverbindliche elektronische Transaktionen im öffentlich-rechtlichen Bereich zu schaffen.

SO Dass der Bund die Rahmenbedingungen für den elektronischen Geschäftsverkehr festlegt und die Einhaltung der technischen und organisatorischen Voraussetzung hierzu überprüft, begrüssen wir. Wir verschliessen uns der Möglichkeit nicht, dass der Geschäftsverkehr mit unseren Grundbuch- und Handelsregisterämtern, und wohl auch den Amtschreibereien als Beurkundungsstellen, in absehbarer Zukunft elektronisch ablaufen könnte. Insbesondere im Tätigkeitsbereich der Betreibungs- und Konkursämter könnte der Einsatz dieser Technologie sinnvoll sein. Allerdings muss es den Kantonen vorbehalten bleiben, den richtigen Zeitpunkt für die Teilnahme am elektronischen Geschäftsverkehr festzulegen. Ihnen wird damit die sehr anspruchsvolle Aufgabe aufgebürdet, elektronische Dokumente sicher und auf sehr lange Dauer abzulegen. Sowohl Handelsregister- wie auch Grundbuchbelege sind während einer unbeschränkten Dauer aufzubewahren. Es wären künftig parallel zwei Belegsysteme zu führen, eines für die Originalbelege auf Papier und das andere für die Belege in elektronischer Form. Zudem müssten erhebliche Informatikinvestitionen vorgenommen werden, um die elektronisch ausgetauschten und digital signierten Buchungsbelege und Geschäftskorrespondenzen wirksam überprüfen zu können (vgl. Begleitbericht Ziff. 15).

TG Die gleichen Gründe, welche das Formerfordernis der öffentlichen Beurkundung rechtfertigen, können im Grundbuchverkehr auch für die Beibehaltung der papiergebundenen Schriftform angeführt werden. Auch bei einem in Schriftform gültigen Erbteilungsvertrag oder einem Dienstbarkeitsvertrag müssen die Parteien in der Regel vor Ort auf Unklarheiten, Schwierigkeiten und rechtliche Konsequenzen hingewiesen und entsprechend beraten werden, was bei einer elektronischen Kommunikation mit dem Grundbuchamt nicht mehr erreicht werden kann. Bei diesen Vertragsarten ist eine verlässliche Grundlage für die nachfolgende Grundbucheintragung ebenfalls unbedingt erforderlich und es sollen nachträgliche Beweisschwierigkeiten über den gewählten Wortlaut verhindert werden können.

Auch nicht beurkundungspflichtige Grundbuchanmeldungen, Löschungsanträge, Pfandfreigaben usw. dürfen in ihren Auswirkungen nicht unterschätzt

werden. Schliesslich führen diese Erklärungen zum dinglichen Vollzug der ihnen zugrundeliegenden Rechtsgeschäfte im Grundbuch. Die elektronische Abgabe von Grundbuchanmeldungen dürfte voraussichtlich zu einer hohen Abweisungsquote führen, weil mit vielen fehlerhaften und mangelhaften Anmeldungen gerechnet werden müsste.

Der Zusammenhang zwischen dem EDV-Grundbuch und der elektronischen Kommunikation mit dem Grundbuch ist unklar. Auf Seite 13 des Begleitberichts zum Entwurf wird für die elektronische Kommunikation mit dem Grundbuchamt vorausgesetzt, dass die entsprechenden Register elektronisch geführt werden. Diese Aussage trifft u.E. nicht zu. Auch wenn ein Grundbuchamt das Grundbuch noch auf Papier führt, können ihm Belege elektronisch eingereicht werden.

Zusammenfassend kann festgehalten werden, dass die elektronische Signatur im Geschäftsverkehr mit dem Grundbuchamt eher Nachteile als Vorteile bringen dürfte. Auch das Kosten-/Nutzenverhältnis dürfte voraussichtlich negativ ausfallen. Die hohe Sorgfaltspflicht und Verantwortlichkeit im Grundbuchverkehr, verbunden mit der extrem stark verankerten Schadenshaftung in Art. 955 ZGB, stehen der vorgeschlagenen Lösung im Wege.

VD Le Conseil d'Etat vaudois prend acte que le projet crée une base légale qui permettra à l'avenir de communiquer par la voie électronique avec les autorités responsables du registre du commerce, du registre foncier et des registres du domaine de la propriété intellectuelle. Il se réjouit du fait que le droit fédéral s'adapte rapidement à l'évolution de la société et de la technique.

VS La modification du code des obligations par l'adjonction d'un article 15a nouveau assimilant la signature électronique à la signature manuscrite lorsqu'elle repose sur un certificat d'un fournisseur de services de certification reconnu constitue une conséquence directe et nécessaire de la LFSél. Les modifications du code civil et du code des obligations aux chapitres du registre foncier et du registre du commerce vont au-delà du cadre restreint de la signature électronique qui reçoit certes une reconnaissance juridique expresse dans ces domaines. La technique rédactionnelle de l'ajout d'une phrase utilisée aux articles 963, 964 et 977 du projet de modification du CCS ne nous semble pas opportune car, faisant école, elle conduirait à un alourdissement considérable des articles existants sur la forme écrite, tant en droit fédéral que cantonal. La clause générale, du type de l'article 15a P-CO, devrait être préférée. Le projet donne une base légale à de futures ordonnances du Conseil fédéral sur les documents électroniques à produire et sur la tenue électronique obligatoire des registres. Cette délégation de compétence normative ne se conçoit qu'à la condition que les cantons soient entendus sur les projets d'ordonnance.

<u>Organisationen / Organisations / Organizzazioni</u>

economiesuisse Wir begrüssen eine weitgehende Ermöglichung des elektronischen Verkehrs mit den Behörden. Der Verkehr mit den Registern, wie er in der Vorlage enthalten ist, kann mithin nur ein erster Schritt darstellen. Dieser Bereich ist zügig auf allen Stufen und für alle Rechtsakte auszubauen. Dies würde allerdings angesichts der verteilt angesiedelten Kompetenzen den Rahmen der heutigen Vorlage sprengen, und wir begrüssen das zweistufige Vorgehen.

EKK La Commission relève les « modestes progrès » apportés dans le domaine des rapports des administrés avec les autorités (cyberadministration). Il apparaît judicieux que l’accès en ligne aux données et registres de l’Institut fédéral de la propriété intellectuelle soit en principe gratuit.

Toutefois, si ce dernier, en concurrence avec le secteur privé, devait décider d'exiger une rémunération pour ce service, la Commission opterait pour une solution prévoyant un accès aux données recherchées le plus simple possible pour l'administré.

SVV Zu begrüssen sind auch die vorgesehenen Änderungen im Registerrecht (Grundbuch, Handelsregister, Topographienregister, Markenregister, Patentregister). Durch die elektronische Führung der Register bieten sich auch elektronische Abfragemöglichkeiten an, was den Geschäftsalltag entscheidend erleichtert.

VSG Un grave problema sarà soprattutto l'armonizzazione della durata di conservazione dei documenti da parte dell'URF, dell'URC e dei prestatori di servizi di certificazione. Nell'ambito del RC i documenti devono essere conservati per dieci anni dalla cancellazione di una ditta, mentre nell'ambito del RF devono essere conservati per sempre. L'art. 23 LFiE prevede che i prestatori di servizio dovranno conservare i certificati elettronici dopo la revoca o l'annullamento di un certificato, senza però specificare per quanto tempo. Se trascorso il termine di conservazione, gli URC/URF necessitassero di tali informazioni, non potrebbero più fare capo al certificato pubblico.
Ripercussioni organizzative e finanziarie su Cantoni e Comuni a seguito dell'introduzione del sistema informatico - sia per ricevere dichiarazioni sia per rilasciare estratti autenticati per via elettronica. Il Cantone dovrà farsi anch'esso promotore quale prestatore di un servizio di certificazione?

322.2 Zivilgesetzbuch / Code civil / Codice civile

322.21 Art. 942 Abs. 3 / Art. 942 al. 3 / Art. 942 cpv. 3

Kantone / Cantons / Cantoni

AG Die vorgeschlagene Revision des ZGB schafft die gesetzliche Grundlage für die rechtliche Anerkennung der elektronischen Signatur im Grundbuchbereich. Anmeldungen, Ausweise über den Rechtsgrund und weitere Belege für die Eintragung, Änderung oder Löschung sollen dem Grundbuchamt (neu) elektronisch eingereicht werden dürfen. Umgekehrt soll das Grundbuchamt Grundbuchauszüge elektronisch signieren können (Art. 949a Abs. 2 lit. b ZGB).
Die Möglichkeit, dass künftig (auch) mit dem Grundbuch elektronisch kommuniziert werden kann, entspricht ohne Zweifel einem wachsenden Bedürfnis. Grundsätzliche Überlegungen veranlassen uns jedoch zu folgenden Bemerkungen:
Im Gegensatz zum Handelsregister lässt das Bundesrecht den Kantonen im Bereich des Grundbuchwesens einen grossen Spielraum (Art. 951 ff. ZGB; Art. 927 ff. OR). Die Folge davon ist, dass man in den Kantonen – teilweise sogar innerhalb deren Grenzen – heute mehrere verschiedene Grundbucheinrichtungen kennt (im Kanton Aargau beispielsweise kantonale Grundbucheinrichtungen sowie das eidgenössische Grundbuch). Der Kanton Aargau führt das Grundbuch heute noch auf Papier. Mit der geplanten Einführung des elektronischen Grundbuches wird eine zweite Art der Grundbuchführung dazukommen. Unseres Erachtens täte der Bundesgesetzgeber gut daran, vorerst im Bereich der Einrichtung und der Führung des Grundbuches bei den einzelnen Kantonen auf einen einheitlichen Standard hinzuwirken, bevor verschiedene Arten von Belegen (Belege auf Papier und elektronisch übermittelte) zugelassen werden.

Sofern die elektronische Kommunikation mit dem Grundbuchamt zugelassen wird, sollte auf Bundesebene zudem geregelt werden, wie die dem Grundbuchamt elektronisch übermittelten Anmeldungen zu registrieren sind. Solange nicht sämtliche Belege (z.B. öffentliche Urkunden) den Grundbuchämtern elektronisch übermittelt werden können, scheint es unumgänglich, dass das Grundbuchamt diese ausdruckt und zusammen mit den auf Papier eingegangenen Belegen archiviert.

Gemäss Art. 942 Abs. 3 ZGB sowie Art. 949a Abs. 1 ZGB soll das Grundbuch nicht nur mit elektronischer Datenverarbeitung, sondern (neu) auch mit „vergleichbarer anderer Datenverarbeitung“ geführt werden können. Was unter letzterer zu verstehen ist, geht aus den Vernehmlassungsunterlagen nicht hervor. Um im Bereich des Grundbuchwesens langfristig einen einheitlichen Standard zu erreichen (bei welchem es sich nur um die elektronische Datenverarbeitung handeln kann), sollte die Zulassung „vergleichbarer anderer Datenverarbeitung“ ausgeschlossen werden. Die Chance, mit der Zulassung der elektronischen Datenverarbeitung gesamtschweizerisch einen einheitlichen Standard in der Grundbuchführung erreichen zu können, sollte nicht vertan werden, indem nun auch wieder „vergleichbare andere Datenverarbeitungen“ zugelassen werden.

BS In Ziff. 221 des Begleitberichtes heisst es : „Die heute in Artikel 949a Absatz 1 ZGB mittelbar enthaltende Aussage, wonach das Grundbuch nicht nur auf Papier, sondern auch mit EDV geführt werden darf, wird vom Entwurf explizit in den Gesetzestext aufgenommen.“ - Dass das Grundbuch nicht nur auf Papier, sondern auch mit EDV geführt werden darf, bedeutet zunächst, dass man es führen darf oder auch nicht. Die Kantone sind aber verpflichtet, das Grundbuch zu führen; sie sind nicht nur ermächtigt. Es bedeutet aber weiter, dass die Kantone diese Pflicht nicht nur durch die Führung des Grundbuches auf Papier erfüllen können, sondern darüber hinaus es zusätzlich auch noch mit EDV, also zweimal, doppelt führen können. Aus dem Zusammenhang ergibt sich, dass das nicht gemeint ist. Die Kantone müssen das Grundbuch führen, und zwar entweder auf Papier oder mit EDV. - Gesetzgebung erfordert die Präzision eines Präzisionsschützen, die Genauigkeit eines Schrotflintenjägers genügt nicht.

Im Registerrecht, insbesondere im Bereich des Grundbuchrechts, gelten seit jeher spezielle Anforderungen an die Form und den Inhalt der Anmeldungen und Belege. So müssen, entgegen der in Art. 11 OR grundsätzlich stipulierten Formfreiheit der Verträge, sämtliche Verträge mindestens in Schriftform abgefasst sein, damit sie auch als Grundbuchbelege anerkannt werden können. Dazu kommt die grosse Anzahl von Verträgen, welche öffentlich zu beurkunden sind. Aufgrund dieser Rahmenbedingungen ergeben sich neue Fragen, wenn zusätzlich zur einfachen Schriftform und der öffentlichen Urkunde als weitere Form eines Beleges die digitale Form möglich wird :

Ist für eine Grundbuchanmeldung die Einheit der Form vorzuschreiben oder darf eine Grundbuchanmeldung Akten sowohl in digitaler Form als auch in öffentlich beurkundeter Form enthalten und wie ist eine solche zweiförmige Grundbuchanmeldung zu behandeln ?

Wie wird auf einen Beleg zurückgegriffen, wenn die Dauer der Zertifizierung abgelaufen ist ? Möglicherweise können diese Fragen erst beantwortet werden, wenn sämtliche dinglichen Eintragungen im EDV-Grundbuch festgehalten sind und auf eine Archivierung der Belege verzichtet werden kann. Weitere Gesetzesänderungen wären somit Voraussetzung.

Zu weiteren Problemen kann sodann die Tatsache führen, dass die Kantone im Bereich der öffentlichen Urkunden die Einführung der elektronischen Form selbständig beschliessen können. Die Frage ist erlaubt, ob das Interesse an einer gesamtschweizerischen einheitlichen Lösung nicht höher zu werten ist, als das Interesse an einer zwar föderalistischen, aber nicht sehr kundenfreundlichen Regelung. Nähere Ausführungen auch zu diesem Punkt wären wünschenswert.
Anders als bei den Grundbuchanmeldungen und den Belegen ist bei der Ausgabe von Grundbuchdaten der Einsatz digitaler Formen unserer Ansicht nach ohne weiteres vorstellbar und zu begrüssen. Da der Interessennachweis in der Regel einfach zu erbringen ist, erreichen viele Auszugsbestellungen unser Grundbuchamt schon heute über das Internet in digitaler Form oder per Faxgerät. Es würde deshalb einem echten Bedürfnis entsprechen, wenn auch die Auszüge aus dem Grundbuch auf digitalem Weg an die Bestellerin oder den Besteller geschickt werden können. Der Verwendungszweck solcher digitaler Auszüge dürfte allerdings eingeschränkt sein, da er nur für die Erstempfängerin oder den Erstempfänger dieselbe Bedeutung haben kann wie ein in Papierform abgegebener, beglaubigter Grundbuchauszug. Dieser kann bekanntlich zum Beispiel an ein Bankinstitut weitergegeben werden.

TG Vgl. zu Art. 949a ZGB / Cf. ad art. 949a CC / Cfr. ad art. 949a CC.

TI La proposta di un nuovo art. 942 cpv. 3 CC sancisce, a giusta ragione, il rispetto dell'autonomia cantonale. L'art. 949a CC (sul quale si fondano gli art. 111 e segg. RRF) consente già ora ai Cantoni di tenere il registro fondiario in forma elettronica. Ogni Cantone deve però poter adeguare la propria legislazione e le proprie strutture in modo autonomo. Tale aspetto è essenziale se si considerano i costi inerenti alla firma elettronica (adattamento apparecchiature informatiche, nuovi programmi, modifiche legislative ed organizzative), che saranno indubbiamente ingenti, per lo meno nei primi tempi.
L'introduzione della firma elettronica, con l'equiparazione di quest'ultima all'autentica di firma e di documenti, imporrà inoltre la modifica di numerose leggi cantonali (in particolare la Legge notarile, il Codice di procedura civile, la Legge di applicazione e complemento del Codice civile) e un cambiamento nell'attività di autentica delle firme, ora devoluta ai notai, ai segretari comunali, alla Cancelleria dello Stato. I Cantoni devono quindi avere il tempo di predisporre gli adeguamenti necessari in funzione delle loro disponibilità finanziarie e delle possibilità concrete di modificare le strutture esistenti nel rispetto delle particolarità locali.

Organisationen / Organisations / Organizzazioni

CP Il est prévu de stipuler que le registre foncier pourra être tenu non seulement sur papier, mais aussi par des moyens électroniques. Nous pensons que cela tient compte de l'évolution technologique.

322.22 Art. 949a

Kantone / Cantons / Cantoni

BL Der Vernehmlassungsentwurf sieht vor, dass es auch im Bereich der Grundbuchanmeldungen möglich sein soll, Anmeldungen auf dem elektronischen Weg vorzunehmen. In diesem Zusammenhang ist wünschenswert, dass eine Koordination der im Bundesrecht enthaltenen formellen Anforderungen an die Grundbuchanmeldungen stattfindet. Es ist widersprüchlich, einerseits strenge Prüfungspflichten hinsichtlich Identität und Verfügungsrecht aufzustellen und andererseits Erleichterungen zu schaffen. Durch die Grundbuchverordnung

muss klargestellt werden, dass sich Grundbuchverwalter und Notare auf eine elektronische Unterschrift verlassen dürfen. Aufgrund des vorgelegten Gesetzesentwurfs und den Erläuterungen dazu gehen wir – insbesondere im Hinblick auf allfällig notwendig werdende Investitionen – davon aus, dass der Entscheid, ob und ab welchem Zeitpunkt elektronische Anmeldungen entgegen genommen werden, beim Kanton liegt.

BS In der amtlichen Vermessung hat sich das Bestehen einer einheitlichen Schnittstelle seit Jahren bestens bewährt. Der gesamtschweizerische Austausch von Grundbuchdaten entspricht bereits heute einem Bedürfnis und wird nach der flächendeckenden Einführung der EDV-Grundbuchführung noch an Bedeutung gewinnen. Wir unterstützen deshalb die Realisierung einer entsprechenden Schnittstelle für das Grundbuch.

FR Nous souhaitons, en ce qui concerne l'art. 949a ch. 3 CC, qu'en cas de définition d'une interface unique au niveau fédéral, l'on tienne compte des systèmes déjà développés par les cantons. Nous pensons, en particulier, aux registres fonciers ou aux systèmes d'information sur le sol, tels les registres des parcelles liés aux paiements directs dans l'agriculture ou les relevés forestiers.

GR Zum vorgesehenen Einsatz der digitalen Signatur und der Zulassung des elektronischen Geschäftsverkehrs im Grundbuchbereich sind Vorbehalte anzubringen. Vorab ist einmal festzustellen, dass der elektronische Geschäftsverkehr mit dem Grundbuchamt nur in einem kleinen Teilbereich der gesamten Grundbuchführung möglich sein wird, weil mit der elektronischen Signatur nur die papiergebundene eigenhändige Unterschrift, nicht aber die Formvorschrift der öffentlichen Beurkundung ersetzt wird. Eine umfassende elektronische Kommunikation mit dem Grundbuchamt wird deshalb in allen beurkundungspflichtigen Fällen nicht möglich sein.

Überlegt man sich die Einführung der digitalen Signatur im Geschäftsverkehr mit dem Grundbuchamt, gilt es, sich die konkreten Verhältnisse vor Augen zu halten. Vielerorts bestehen noch kantonale Grundbucheinrichtungen, die durch die Anlage des Eidgenössischen Grundbuches ersetzt werden sollten. Nach der geltenden gesetzlichen Regelung kann das Grundbuch mit elektronischer Datenverarbeitung geführt werden. Dieses EDV-Grundbuch ist in der Schweiz jedoch bei weitem noch nicht angelegt worden. In einigen Kantonen sind noch nicht einmal die Ausführungsgesetzgebungen hierfür geschaffen, geschweige denn die Datenerfassungen gemacht worden. Wie in anderen Kantonen, so bestehen auch im Kanton Graubünden auf einzelnen Ämtern bis zu fünf verschiedene Grundbucheinrichtungen, nämlich Kauf- und Pfandprotokolle, Liegenschafts- und Servitutenregister, Eidgenössisches Grundbuch in Folianten, Eidgenössisches Grundbuch im Faltsystem auf Blättern und EDV-Grundbuch. Zu diesen unterschiedlichen Grundbucheinrichtungen sollen sich nun neu auch noch zwei verschiedene Arten von Belegen gesellen, nämlich solche auf Papier und elektronisch übermittelte. Die Einführung des elektronischen Geschäftsverkehrs hat diesen besonderen Umständen Rechnung zu tragen.

Zu Abs. 2: Sofern die elektronische Kommunikation mit den Grundbuchämtern zugelassen wird, erscheint es erforderlich, auf Bundesebene in den Ausführungsbestimmungen eine Regelung zu schaffen, wie diese elektronisch eingereichten Anmeldungen, Ausweise über den Rechtsgrund und weitere Belege beim Grundbuchamt registriert werden.

Der Rang der dinglichen Rechte bestimmt sich nach dem Zeitpunkt der Tagebuchaufnahme. Da neu auch elektronisch übermittelte Grundbuchanmeldungen zugelassen werden sollen, muss geregelt werden, wie diese Anmeldungen in

das (auf Papier oder mittels EDV geführte) Tagebuch aufgenommen werden. Genügt bereits der Eingang der elektronischen Anmeldung per E-Mail oder bedarf es zusätzlich noch einer Einschreibung in das Tagebuch. Die grosse rechtliche Bedeutung des Tagebuchs erfordert eine gesetzliche Regelung im ZGB.

Zu Abs. 3: Wegen der allerorts entstehenden Bodeninformationssysteme (LIS, GIS etc.) besteht ein grosses Bedürfnis, dass der Bund eine einheitliche Schnittstelle festlegt. In Berücksichtigung der grossen praktischen Bedeutung und der vorauszusehenden Kosteneinsparungen beantragen wir, von einer blossen Kann-Bestimmung abzusehen und den Bundesrat zu verpflichten, eine einheitliche Schnittstelle festzulegen.

NE La reconnaissance de la signature électronique en matière de registre foncier est tout à fait imaginable et va même faciliter des opérations avec les banques notamment et les particuliers dans des actes sous seing privé.

Il faut cependant faire remarquer que le caractère authentique de certains actes et le fait qu'ils concernent le plus souvent plusieurs personnes ou ayant droits demeurent des obstacles importants.

SG Wir beantragen, Art. 949a Abs. 2 Bst. b in einen eigenen Absatz zu fassen und die Bst. a und g zusammenzufassen.

Begründung: Mit Ausnahme von Bst. b betrifft Art. 949a Abs. 2 die Führung des EDV-Grundbuchs, Bst. a und g im Allgemeinen, Bst. c bis f im Besonderen. Art. 949a Abs. 2 Bst. b hingegen betrifft die rechtliche Anerkennung der elektronischen Signatur im Grundbuchbereich.

Wir beantragen, Art. 949a Abs. 3 wie folgt zu formulieren: „Der Bundesrat *legt* namentlich für ... eine einheitliche Schnittstelle fest."

Begründung: Aus Gründen der Kundenfreundlichkeit und der Effizienz in der Verfahrensabwicklung ist die rechtliche Anerkennung der elektronischen Signatur im Grundbuchbereich gesamtschweizerisch zu koordinieren.

TG Zu den einzelnen Bestimmungen ist festzuhalten, dass der in Art. 942 Abs. 3 sowie Art. 949a Abs. 1 ZGB verwendete Begriff der „vergleichbaren anderen Datenverarbeitung" unverständlich ist. Es wird nirgends erläutert, was darunter zu verstehen ist. Die Bestimmung von Art. 949a Abs. 3 ZGB ist wegen der grossen praktischen Bedeutung wichtig und sollte deshalb nicht nur in der Kann-Formulierung ins Gesetz aufgenommen werden.

TI Lo scrivente Consiglio ritiene che sia indispensabile precisare quando la trasmissione del documento elettronico esplica effetto giuridico (con riferimento all'art. 972 CC e all'art. 14 del Regolamento sui registro fondiario). Il Regolamento sui registro fondiario dovrà se del caso essere adeguato alle nuove esigenze poste dall'uso della firma elettronica.

Il principio della parità di trattamento tra gli utenti richiede che il momento in cui il documento elettronico perviene all'ufficio del registro corrisponda all'apertura del messaggio elettronico negli orari di ufficio dell'amministrazione destinataria, così da non discriminare gli utenti che continuano a usare i metodi tradizionali.

La Confederazione deve se del caso modificare l'art. 53 RRF per consentire, se così Io ritiene opportuno, il rilascio della cartella ipotecaria in forma elettronica. Si pongono tuttavia rilevanti problemi di sicurezza, che non devono essere sottovalutati, vista l'importanza del titolo e il suo ruolo nel mercato immobiliare.

Il registro fondiario conserva i documenti giustificativi a tempo indeterminato, in modo da consentirne la visione ai terzi e ai tribunali anche a distanza di decenni. È pertanto necessario armonizzare l'obbligo di conservare i dati del prestatore di servizi di certificazioni (art. 23 LRE) con le necessità di archiviazione

del registro fondiario. Il documento elettronico dovrebbe poter essere accessibile in ogni momento (si potrebbe pensare a tecniche per „sviluppare“ il supporto di dati in modo da trascrivere i dati contenuti nel documento elettronico crittografato).

ZG Im BGES selbst wird der elektronische Verkehr mit dem Grundbuchamt nicht erwähnt. Dass die elektronische Signatur auch im Verhältnis zum Grundbuchamt Geltung haben soll, ergibt sich vielmehr aus den vorgeschlagenen Änderungen der Art. 949a Abs. 2 Bst. b, 963 Abs. 1, 964 Abs. 1 und 977 Abs. 1 ZGB. Nach dem neuen Art. 949a Abs. 2 Bst. b ZGB sollen die Voraussetzungen, unter denen Anmeldungen, Ausweise über den Rechtsgrund und weitere Belege für die Eintragung, Änderung oder Löschung beim Grundbuchamt eingereicht werden dürfen und Auszüge anerkannt werden können, vom Bundesrat geregelt werden. Da ein Verordnungsentwurf noch nicht existiert, ist die Ausgestaltung der zukünftigen Regelung des elektronischen Verkehrs mit dem Grundbuchamt offen, was die Stellungnahme erschwert.
Wie bereits bei der Einführung des EDV-Grundbuches, handelt es sich auch bei der Realisierung des elektronischen Geschäftsverkehrs mit dem Grundbuchamt um ein Projekt, das die Grundbuchführung revolutioniert. Wir bezweifeln, dass diese Änderungen vom Grundbuchamt Zug, welches sich in den kommenden Jahren intensiv der Einführung des eidgenössischen Grundbuches widmen muss, im gegenwärtigen Zeitpunkt verkraftet werden könnten.
Anders als in vielen anderen Bereichen bildet bei Grundbuchgeschäften die Schnelligkeit des Austausches von Willenserklärungen zwischen den Vertragsparteien bzw. zwischen Privaten und dem Grundbuchamt kein wesentliches Kriterium. Im Gegenteil: Die Tragweite der mit dem Abschluss und Vollzug eines Grundbuchgeschäftes verbundenen Wirkungen hat den Gesetzgeber veranlasst, die beteiligten Parteien vor Übereilung zu schützen, namentlich indem er Verträge über dingliche Rechte dem Erfordernis der öffentlichen Beurkundung unterstellt hat. Bei Verträgen über dingliche Rechte an Grundstücken handelt es sich des weiteren nicht um Verträge, welche vom durchschnittlichen Kunden besonders häufig abgeschlossen werden. Der praktische Nutzen des elektronischen Verkehrs mit dem Grundbuchamt ist für denselben daher relativ.
Für die Allgemeinheit von Bedeutung dürfte vor allem die Bestellung bzw. Lieferung von Grundbuchauszügen auf elektronischem Wege sein. Der Gesetzesentwurf eröffnet die Möglichkeit der elektronischen Unterzeichnung solcher Grundbuchauszüge durch das Grundbuchamt (Art. 949a Abs. 2 Bst. b E-ZGB), was wir begrüssen. Allerdings setzt der Versand von Grundbuchauszügen via Internet voraus, dass verschiedene Aspekte, namentlich solche der Datensicherheit (Chiffrierung), vorgängig gelöst werden.

<u>Organisationen / Organisations / Organizzazioni</u>

CP Nous trouvons ici la base légale pour la reconnaissance juridique de la signature électronique dans le domaine foncier. Cela est tout à fait souhaitable du moment que le registre peut être tenu de manière électronique.

VSG Secondo l'art. 972 CC, i diritti reali nascono e ricevono grado e data dal momento dell'iscrizione nel libro mastro; il loro effetto risale al giorno dell'iscrizione nel giornale a condizione che siano in pari tempo prodotti i documenti giustificativi prescritti dalla legge. L'art. 14 RRF prevede che ogni iscrizione deve essere riportata a libro giornale non appena giunta; in altre parole l'ufficiale esegue un'iscrizione cronologica a libro giornale (R. Pfäffli, Der Ausweis für die Eigentumseintragung im Grundbuch, Langenthal 1999, pag. 29 ss.).

Il progetto di legge non prevede di specificare, modificando l'art. 972 CC, il momento dell'effetto delle richieste.
L'art. 13 cpv. 4 RRF invece precisa questo determinato momento quando la richiesta è iscritta nel giornale con la data e il momento della comunicazione telefonica o elettronica (posta elettronica, fax), ossia quando il documento arriva al destinatario (R. Pfäffli, Der Ausweis für die Eigentumseintragung im Grundbuch, Langenthal 1999, pag. 30 e nota 122 e pag. 58).
Domanda: il momento di „arrivo" per via elettronica (non per telefono) è da intendere come:
1) momento della ricezione nella „bucalettere del computer (Inbox)" dell'URF (quindi anche fuori orario d'ufficio, p.es: a mezzanotte) o
2) momento della ricezione effettiva, ossia dell'apertura del messaggio da parte del responsabile RF (dunque in orario d'ufficio)?
È auspicabile che comunque vi sia univocità nello stabilire il momento dal quale la richiesta esplica i propri effetti, tenendo conto del contenuto della norma già introdotta (art. 13 RRF).
C'è comunque da chiedersi se l'inoltro delle richieste e dei contratti ai rispettivi uffici debba essere disciplinato entro fasce orarie precise (aperture degli uffici) o se potrà essere lasciato libero. Immaginiamo le difficoltà o i conflitti che sorgeranno tra richieste inviate elettronicamente tra sabato e domenica e quelle cartacee inviate il venerdì sera (fallimenti, restrizioni ecc.). Non da ultimo anche eventuali black-out elettronici o altre difficoltà analoghe.
I documenti giustificativi sulla base dei quali sono fatte le iscrizioni devono essere debitamente allegati e conservati (art. 948 cpv. 2 CC). Il tenore di questa norma rimane invariato: le dichiarazioni, i documenti, le istanze potranno essere stampate o conservate su dischetti, schede o microfiches. Uno dei punti da chiarire sarà appunto la sicura archiviazione dei dati elettronici e la loro costante verifica, la loro protezione e integrità (pag. 13 rapporto esplicativo, prospettive in generale; non è escluso che in futuro si potranno apportare modifiche indebite senza lasciare tracce).
Sicurezza sull'identità delle persone che postulano mutamenti a registro (istanti), in particolare per quanto concerne la loro facoltà di disporre/titolarità del diritto da iscrivere, modificare, cancellare.
Implicazioni a livello pratico per la tenuta a giorno del registro fondiario e problematiche relative al registro fondiario federale e cantonale.
a) Si deduce che qualsiasi richiesta sottoscritta dal proprietario o avente diritto la cui firma è stata certificata conforme deve essere accettata dall'ufficiale dei registri. Ciò equivarrà all'autentica posta da un notaio mediante la quale l'ufficiale dà seguito all'art. 15 cpv. 2 e cpv. 3 del RRF? Analogo ragionamento per le procure.
b) L'Ufficio del registro fondiario potrà in futuro rilasciare le cartelle ipotecarie, titoli ipotecari o di rendita fondiaria con le nuove modalità che regolano il commercio elettronico e la firma elettronica? Basterà la firma elettronica per adempiere la prescrizione dell'art. 53 cpv. 1 del RRF? Vedi mozione Schiesser 19 marzo 1998.
c) Quale forma dovrà rivestire la firma utilizzabile nell'ambito del nostro settore? firma elettronica - molto prossima alle nostre esigenze - o firma digitale.
d) II riconoscimento internazionale (con chiavi di prestatori di servizio esteri riconosciuti) supplirà in tutto e per tutto la verifica delle specifiche competenze in materia di autenticazione delle firme (postilla dell'Aja, legalizzazioni tramite Ambasciate e Consolati)?

e) La decisione di rifiuto di una richiesta eseguita con i nuovi criteri adempie tutte le formalità previste dalla legge e cioè: intimazione, comunicazione agli aventi diritto, termini d'impugnazione, ecc.?
La revisione dell'art. 949a CC pone le basi per il riconoscimento della firma elettronica nel settore del registro fondiario. Ne consegue che l'autorità federale non deve obbligare imperativamente i Cantoni ad utilizzare questa forma, ma dovrà essere una libera scelta. Ciò permetterebbe inoltre l'introduzione dei nuovi sistemi in modo più armonioso e ponderato.
Inconfutabile il fatto che si rendono necessarie, per l'applicazione della firma digitale/elettronica, delle condizioni prioritarie di sicurezza che garantiscano all'ufficio i dati trasmessi (riservatezza, integrità e prova dell'invio) e la certezza circa l'autore (titolare della chiave pubblica e privata).
Tutto ciò premesso, richiamate le nostre considerazioni e osservazioni di cui alla presente, viste le argomentazioni e chiarificazioni addotte dal Dipartimento, siamo di principio a preavvisare favorevolmente la prospettata modifica legislativa.

SVV Jede Möglichkeit mit den Registerämtern elektronisch zu korrespondieren, vereinfacht den Geschäftsalltag und ist zu begrüssen. Insofern ist an den Bestimmungen zum Grundbuch aus Sicht der Versicherungswirtschaft nichts einzuwenden. Fraglich ist lediglich, inwiefern aus elektronischen Auszügen die Historie der Belastungen eines Grundstücks noch hervorgehen wird. Sollte lediglich der Status quo ausgewiesen werden, könnten im Rahmen des Hypothekargeschäfts wichtige Informationen verloren gehen. Wir stellen deshalb den Antrag, dass dieser Punkt bei der Ausarbeitung der bundesrätlichen Verordnung berücksichtigt wird.

322.23 Art. 963 Abs. 1 / Art. 963 al. 1 / Art. 963 cpv. 1

Organisationen / Organisations / Organizzazioni

CP Nous souscrivons à ces modifications.

322.24 Art. 964 Abs. 1 / Art. 964 al. 1 / Art. 964 cpv. 1

Organisationen / Organisations / Organizzazioni

CP Vgl. zu Art. 963 Abs. 1 ZGB / Cf. ad art. 963 al. 1 CC / Cfr. ad art. 963 cpv. 1 CC.

322.25 Art. 977 Abs. 1 / Art. 977 al. 1 / Art. 977 cpv. 1

Kantone / Cantons / Cantoni

SG Wir beantragen, Art. 977 Satz 1 wie folgt zu formulieren: „Berichtigungen darf der Grundbuchverwalter ohne schriftliche Bewilligung der Beteiligten nur auf Verfügung des *Gerichtes* vornehmen."
Begründung: Angleichung der Formulierung an den Sprachgebrauch des ZGB (vgl. dazu AS 1999 1143).

Organisationen / Organisations / Organizzazioni

CP Vgl. zu Art. 963 Abs. 1 ZGB / Cf. ad art. 963 al. 1 CC / Cfr. ad art. 963 cpv. 1 CC.

322.3 Obligationenrecht / Code des obligations / Codice delle obbligazioni

322.31 Art. 15a

Kantone / Cantons / Cantoni

BE Gemäss vorliegendem Entwurf soll die Anerkennung der Anbieterinnen von Zertifizierungsdiensten freiwillig sein. Art. 15a E-OR sieht indes vor, dass nur diejenige elektronische Signatur der eigenhändigen Unterschrift gleichgestellt ist, die auf einem Schlüsselpaar beruht, das von einem anerkannten Zertifizierungsdiensteanbieter zertifiziert worden ist. Unseres Erachtens scheint es fraglich, ob den Konsumentinnen und Konsumenten ein Zweiklassenzertifizierungssystem zugemutet werden darf. Diese werden in der Regel nicht erkennen, dass nicht alle, sondern nur die von einer nach dem vorliegenden Gesetz anerkannten Anbieterin zertifizierten Signaturen die Rechtsfolgen gemäss Obligationenrecht und Bundesgesetz über die elektronische Signatur nach sich ziehen. Wünschbar wäre deshalb, eine Pflicht zur Anerkennung der Anbieterinnen von Zertifizierungsdiensten festzulegen und die Folgen einer Nichtanerkennung zu regeln. Allerdings dürfte es in der Praxis schwierig sein, bereits im Markt präsente Anbieterinnen nicht mehr zuzulassen, zumal die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift für die Konsumentinnen und Konsumenten nicht auf allen Gebieten gleich wichtig sein dürfte.

BS Die Bestimmungen des Bundesgesetzes über den Konsumkredit vom 8. Oktober 1993 sind erlassen worden, um im Rahmen der Übernahme des acquis communautaire des Rechts der EG im Hinblick auf den Beitritt der Schweiz zum Europäischen Wirtschaftsraum die Richtlinie Nr. 87 / 102 des Rates vom 22. Dezember 1986 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über den Verbraucherkredit, revidiert durch die Richtlinie Nr. 90 / 88 des Rates vom 22. Februar 1990 den Konsumenten gegen missbräuchliche Bedingungen bei der Kreditgewährung und ähnlichen Geschäften zu schützen. Zu diesem Schutzzweck wurde die schriftliche Vertragsform verlangt. Es sollen Konsumentinnen und Konsumenten vor übereilter Verschuldung, daraus folgender Abgleitung in die Fürsorgeabhängigkeit und Verelendung bewahrt werden. Wenn durch das Gesetz über die elektronische Signatur die Möglichkeit geschaffen werden soll, auch einen Konsumkreditvertrag elektronisch abzuschliessen, was in Ziff. 142.2 noch besonders hervorgehoben wird, dann liegt hier ein widersprüchliches Verhalten vor.
In Ziff. 122 heisst es, dass das Gesetz ausnahmsweise den Grundsatz der Formfreiheit durchbricht, dass es dabei meist um den Schutz des Schuldners vor dem Eingehen übereilter vertraglicher Verpflichtungen (Übereilungsschutz) geht. Der Konsumentenschutz ist der klassische Fall, eine solche Ausnahme zu machen. Ziff. 5 des Begleitberichts weist darauf hin, dass auch das europäische Recht die Möglichkeit gibt, Ausnahmen zu machen und auszuschliessen, dass ein Vertrag auf elektronischem Wege geschlossen wird. Von dieser Möglichkeit sollte Gebrauch gemacht werden.

GE L'un des objectifs importants du projet, qui est d'assimiler la signature électronique à la signature manuscrite, s'effectuerait par une modification du code des obligations (art. 15a nouveau). Dès le résumé du rapport explicatif, il est précisé que ce projet traite essentiellement des questions de droit privé, qu'il se limite, en matière de cyberadministration, à régler la simple transmission électronique de données, et que des questions relevant de la procédure (telles que l'acceptation du dépôt d'un mémoire ou de la notification d'une décision par la

voie électronique) seront réglées par d'autres lois. Or, il nous apparaît que, à tout le moins faute de disposition de droit public cantonal spécifique, le nouvel art. 15a CO pourrait bien avoir une portée beaucoup plus large. Traitant de la question pour le droit des contrats (parce que les art. 12 ss. CO s'inscrivent dans ce cadre), le projet de modification n'en serait pas moins valable pour l'ensemble des manifestations de volonté soumises au droit privé, en vertu de l'art. 7 CCS, et même pour l'ensemble des manifestations de volonté contenues dans des décisions administratives et des actes de procédure, dans la mesure où la législation de droit public pertinente se bornerait à exiger la „forme écrite“, notion interprétée logiquement en référence aux art. 12 et suivants CO. Ce résultat n'est pas forcément malheureux, mais il faut en être conscient et rechercher les cas dans lesquels des dérogations explicites devraient être apportées en droit public cantonal, ne serait-ce que transitoirement en attendant que les conditions techniques et organisationnelles d'application de cette nouvelle législation soient mises en place. Nous estimons fondamental que le législateur fédéral ait une réflexion approfondie à ce sujet, car il ne paraît pas sain que la résolution de ces questions essentielles soit laissée à la seule responsabilité de la jurisprudence ou de la pratique administrative.

Afin de mieux souligner l'assimilation visée de la signature électronique avec la signature manuscrite, il semblerait préférable de remodeler les art. 14 et suivants plutôt que d'insérer un art. 15a CO faisant suite à un art. 15 CO sur les marques pouvant remplacer la signature et même à un art. 14, al. 3 sur la portée d'une signature manuscrite apposée par des aveugles. En bonne technique législative, les principes doivent être réglés avant les exceptions**.** Or, le principe serait en l'occurrence celui d'un traitement égal des signatures manuscrite et électronique; il pourrait faire l'objet d'un art. 14 recevant une nouvelle teneur. Puis il conviendrait de régler les cas d'exception dans un art. 15 remodelé, sans omettre, au surplus, de vérifier que ces exceptions puissent bien s'appliquer tant à la signature manuscrite qu'à la signature électronique (ou, à défaut, en prévoyant les différences qui s'imposeraient).

JU Sur son principe, le Gouvernement de la République et Canton du Jura peut souscrire à l'assimilation de la signature électronique à la signature manuscrite. Cela suppose toutefois que les parties au contrat puissent avoir une entière confiance dans les certificats qui seront délivrés et qui permettront d'établir le lien, en définitive, avec une personne physique. Or, le projet de loi sur la signature électronique vise précisément à créer un cadre juridique permettant d'instaurer la confiance nécessaire à la promotion du commerce électronique.

SO Strafrechtliche Aspekte: Laut Ziffer 142.2 des Begleitberichts zum Entwurf des BGES soll das neue Bundesgesetz die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift bringen. Das trifft allerdings unter strafrechtlichen Gesichtspunkten nicht zu. Die eigenhändige Unterschrift wird gefälscht, während die elektronische Signatur entweder erschlichen (Zertifikat), gestohlen (Geheimschlüssel) oder geknackt (Zugriffscode) wird.

TG Art. 15a OR ist der eigentliche Kern der Revision. Mit dieser Bestimmung wird die digitale Signatur generell der eigenhändigen Unterschrift gleichgesetzt, womit nicht nur Verträge, die der schriftlichen Form bedürfen, auf elektronischem Weg geschlossen werden können, sondern generell elektronische Dokumente „unterschrieben“ werden können. Dies dürfte vor allem im Bereich der provisorischen Rechtsöffnung bald Bedeutung erlangen. Auch wenn bereits heute ohne digitale Signatur verpflichtende Erklärungen elektronisch übermittelt

werden können, ist ihre Beweiskraft insofern eingeschränkt, als im Bestreitungsfall der Nachweis in einem ordentlichen Beweisverfahren nötig ist.

TI Ci sembra che l'art. 15a CO si riferisca alla forma scritta prevista dalla legge (art. 12 segg. CO) e ai casi in cui le parti hanno scelto tale forma, anche se non obbligatoria, come condizione di validità delle loro pattuizioni (art. 16 CO). Gli altri casi sfuggono per contro alla legge. Si tratta in particolare di tutti i contratti che possono essere conclusi oralmente, ma che le parti scelgono di stipulare in forma scritta come mezzo di prova. Rimangono per contro invariate tutte le disposizioni sull'atto pubblico.

VD S'agissant du nouvel art. 15a du Code des obligations, le Conseil d'Etat vaudois émet certaines réserves. D'une part, le champ d'application de cette nouvelle disposition paraît trop restreint et, d'autre part, sa rédaction pourrait poser certains problèmes d'eurocompatibilité.

Ce nouvel article instaure une équivalence entre la signature manuscrite et la signature électronique. Comme celle relative aux conséquences d'une utilisation abusive d'une clé électronique (art. 17), cette disposition devrait, par souci de cohérence, être comprise dans le paquet des modifications du Code des obligations prévues par l'avant-projet de loi sur le commerce électronique.

Relevons en outre qu'en disposant que la signature électronique est assimilée à la signature manuscrite lorsqu'elle repose sur un certificat d'un fournisseur de services de certification reconnu au sens de la loi fédérale sur la signature électronique, cette nouvelle disposition paraît trop restreinte.

Il découle de la directive européenne que la question de l'assimilation de la signature électronique à l'écrit ne devrait pas dépendre de la question de savoir si le certificat a été délivré par un fournisseur accrédité ou non mais si la fonction propre à l'écrit est réalisée par le mécanisme technologique utilisé.

Par ailleurs, en se fondant sur la seule notion de signature, le projet apparaît également trop restreint et semble pouvoir faire obstacle à l'introduction de nouvelles technologies propres à respecter les fonctions de l'écrit.

En résumé, l'art. 15a nouveau du Code des obligations risque de susciter certains problèmes juridiques dès lors qu'il n'est pas tout à fait conforme à la Directive et qu'il risque ainsi de se heurter aux droits des pays voisins qui reconnaîtront les signatures électroniques dès l'instant où elles respectent les fonctions de l'écrit, sans être nécessairement le fait du titulaire d'un certificat délivré par un fournisseur accrédité.

Organisationen / Organisations / Organizzazioni

Briner Die Einordnung als Art. 15a ist diskutabel. Wesentlicher scheint uns, dass sachlich wenig verständlich ist, weshalb die Signatur nur einer eigenhändigen Unterschrift gleichgestellt sein soll, wenn „ein Vertrag durch elektronischen Datenaustausch abgeschlossen“ wird. Damit wird die Anwendung völlig unnötig eingeschränkt. Es genügt ja, wenn nach vorangegangenem „gewöhnlichem“ Datenaustausch der sich Verpflichtende eine elektronische Erklärung „Ich bin einverstanden“ elektronisch signiert. Weder muss es sich notwendigerweise um einen Vertrag handeln, noch muss der Vertrag selber „elektronisch abgeschlossen“ werden. Auch eine elektronische, elektronisch signierte Erklärung „Ich anerkenne den Schadensbetrag von CHF xyz“ sollte erfasst werden.

Clusis L'étendue de l'assimilation, dans certaines situations, de la signature électronique à la signature manuscrite fait l'objet d'un certain nombre de critiques. Il faut relever que l'introduction proposée par le Projet d'un nouvel art. 15a du Code des obligations viole également le principe de la neutralité

technologique. Sa formulation actuelle est en effet la suivante : „Lorsqu'un contrat est conclu par un échange de données électroniques, la signature électronique est assimilée à la signature manuscrite au sens de l'article 14, lorsqu'elle repose sur un certificat d'un fournisseur de services de certification reconnu au sens de la loi fédérale sur la signature électronique“. Ainsi, tout mécanisme d'authentification autre que la cryptographie asymétrique est exclu. C'est dire que des systèmes comme l'examen des empreintes digitales ou de la rétine, par exemple, ne seraient pas considérés comme étant suffisamment sûrs pour que cette assimilation soit reconnue.
Il paraît donc essentiel de modifier, sur ce point déjà, le projet d'art. 15a du Code des obligations, en faisant, par exemple, référence à *„tout procédé de signature électronique réglementé par la loi fédérale sur la signature électronique“.*
Outre la question du non-respect du principe de la neutralité technologique évoquée ci-dessus, le Projet du nouvel art. 15a du Code des obligations est critiquable dans la mesure où la formulation actuelle ne vise que la question de l'assimilation de la signature électronique à la signature manuscrite, qui plus est dans le cadre particulier de la conclusion d'un contrat. Or, la problématique du formalisme en droit suisse englobe non seulement la question de la signature mais également la question de l'écrit et non seulement la question des contrats mais également celle de l'ensemble des actes juridiques.
Le choix de se limiter à la question de la signature dans le cadre de contrats conclus par voie électronique est pourtant délibéré de la part des auteurs du projet, à en croire le rapport explicatif (ch. 142.2). Or, il ne paraît simplement pas judicieux de laisser au juge, voire aux autorités administratives la possibilité de décider, sans avoir l'assurance d'une pratique uniforme, si cet art. 15a CO doit être appliqué par analogie à des situations où la signature n’est pas exclusivement visée ainsi qu’à des hypothèses où seul un acte juridique doit revêtir la forme écrite (ou la simple notification d'une information) et non pas un contrat.
Même à considérer que cette disposition ne devrait d'ailleurs pas être modifiée sur ce point, il s'agirait néanmoins de préciser si la signature électronique, pour être assimilée à la signature manuscrite, doit reposer sur un certificat d'un fournisseur de services de certification reconnu qui soit également délivré au sens de la loi fédérale sur la signature électronique. En effet, le projet offre la possibilité à des fournisseurs de services de certification reconnus de délivrer des certificats qui eux, ne le seraient pas, ce qui priverait notamment ceux qui les utilisent du bénéfice de la protection des clauses de responsabilité figurant dans le Projet.
Par ailleurs et toujours en rapport avec la question de l'assimilation de la signature électronique, de nombreuses critiques se sont déjà élevées en ce qui concerne l'absence d'obligation, pour les fournisseurs de services de certification, de délivrer des services de „time-stamping“. Il faut en effet rappeler que la durée de validité d'un certificat électronique est limitée et peut être révoquée en tout temps. Ainsi, pour que la signature électronique reposant sur un certificat valable puisse être assimilée à une signature manuscrite au sens du projet d'art. 15a nouveau du Code des obligations, il s'agirait nécessairement d'exiger qu'elle soit accompagnée d'un tampon temporel pouvant attester du moment auquel la signature est intervenue. En l'absence d'une telle indication, le signataire pourrait en effet prétendre que la signature est intervenue ultérieurement à la révocation du certificat.

CP Cette disposition reconnaît la signature électronique et l'assimile à la signature manuscrite. Cette norme est donc centrale puisqu'il en découle de nombreuses conséquences et nous l'approuvons pleinement.

economiesuisse In Fachartikeln wurde in jüngster Zeit verschiedentlich darauf hingewiesen, dass Privatpersonen nur in ausgewählten Fällen auf die letztlich aufwendige elektronische Unterschrift angewiesen sein werden. Es ist richtig und wird auch im Vernehmlassungsbericht ausgeführt, dass aufgrund der Formfreiheit des schweizerischen Vertragsrechts in weiteren Bereichen auch ohne formelle Regelung der elektronischen Schriftform Verträge in elektronischer Form abgeschlossen werden können. Die Entwicklung der Informationsgesellschaft ist bereits in vollem Gange und hängt nicht von der geforderten Anerkennung der elektronischen Unterschrift ab. Letztere ist nur ein – allerdings symbolträchtiges – Element in der ganzen Entwicklung. Dies bedeutet jedoch nicht, dass daraus ein fehlender Bedarf der Gleichstellung der elektronischen Unterschrift mit der handschriftlichen Unterschrift abgeleitet werden darf. Die Schriftform ist für zahlreiche Vorgänge vorgeschrieben und nicht zuletzt gilt dies für vorvertragliche Informationspflichten (z.B. im Versicherungsbereich) oder Abklärungen (z.B. Kontoeröffnung bei Banken).

Wir erachten es als richtig, dass die Anpassung mit einer Änderung des Obligationenrechts vorgenommen wird, ohne alle Einzelgesetze, die von den Formvorschriften betroffen sind, einzeln auch abzuändern. Wir gehen davon aus, dass auch all diese Anpassungen mit der heutigen Vorlage abgedeckt sind (analog etwa dem Bundesgesetz über den Fristenlauf an Samstagen). Entsprechend muss klargestellt sein, dass mit der Einführung der gesetzlichen Anerkennung der elektronischen Unterschrift gleichzeitig das Kriterium der „Schriftform“ in allen Rechtsgebieten erfüllt ist. Dies muss insbesondere auch für einseitige Erklärungen gelten.

In Anbetracht der Tatsache, dass Art. 13 bis 15 OR nicht nur auf Verträge, sondern auf sämtliche Rechtsgeschäfte und auch im öffentlichen Recht anwendbar sind, erscheint der Wortlaut in Art. 15a VE-OR als unnötig eng formuliert („Wird ein Vertrag durch elektronischen Datenaustausch abgeschlossen....“). Insbesondere im Versicherungsbereich gibt es eine Fülle von rechtsgeschäftlichen Erklärungen, die aus Gründen der Rechtssicherheit (Beweiskraft, Fristen) der Schriftlichkeit bedürfen. Soweit eindeutig feststellbar ist, dass sich die Identifizierung „Unterschrift“ auf den Inhalt der Erklärung erstreckt, kann die elektronische Übermittlung der papierenen gleichgestellt werden. Entsprechend sollte Art. 15a wie folgt gefasst werden: *„Der eigenhändigen Unterschrift nach Art. 14 gleichgestellt ist die elektronische Signatur, wenn sie auf dem Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des vorliegenden Gesetzes beruht.“*

EKK La Commission fédérale de la consommation souligne tout particulièrement le nouvel art. 15a CO. Il est en effet important que la signature électronique soit enfin assimilée à la signature manuscrite au sens de l’art. 14 CO. Cette nouvelle disposition ne pourra que contribuer à l’essor des transactions électroniques pour lesquelles la loi exige la forme écrite.

Enfin, la Commission se plaît à relever que le projet va au-delà des exigences du droit européen telles que contenues à l’art. 9 de la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l’information, et notamment du commerce électronique, dans le marché intérieur.

FGSec Die Begriffe „digitale Signatur“ / „elektronische Signatur“ werden inkonsistent verwendet. Die Anerkennung ist gleichgestellt, nicht die Unterschrift.

Es wurde vergessen, dass eine „anerkannte Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes” auch andere Arten von Zertifikaten ausstellen kann, z.B. Test-Zertifikate. Diese sind nicht für eine Verwendung vorgesehen, welche eine Gleichstellung zur Handsignatur erlauben würde. Wir vermissen ein Äquivalent zur EU-Direktive bzgl. Fortgeschrittene elektronische Signatur (Advanced Electronic Signature), Qualifiziertes Zertifikat (Qualified Certificate) und „Sichere Signaturerstellungseinheit“ (Secure Signature Creation Device). Nicht nur der CSP, sondern auch Zertifikat, Signatur sowie sichere Signaturerstellungseinheit müssen dem BGES entsprechen.

ISACA Contrairement à une signature manuscrite, un certificat a une durée de vie qui peut être limitée. Un certificat peut être échu, suspendu ou annulé. La datation (time stamping) de l’échange de données électroniques constitue donc un élément constitutif de la signature électronique.

Compléter l'art. 15a : „…. lorsque l’échange est daté de manière appropriée et que la signature repose sur un certificat d’un fournisseur de services de certification reconnu au sens de la loi fédérale sur la signature électronique“. Régler la question de la datation dans les dispositions d’exécution du Conseil fédéral, en veillant aux problèmes liés aux fuseaux horaires et au changement d’heures saisonnier.

Jeune Barreau vaudois Wie / Comme / Come Clusis.

KPMG Ziel der neuen Gesetzgebung muss es sein, in Zukunft eine formgültige Unterschrift genau so gut mittels digitaler Signatur als mittels eigenhändiger Unterschrift leisten zu können. Rechtsnormen, die zu einer unterschiedlichen rechtlichen Würdigung der handschriftlichen Unterschrift einerseits und der elektronischen Unterschrift andererseits führen, würden die Rechtssicherheit im Zusammenhang mit unterzeichneten Dokumenten in Frage stellen. Es ist uns deshalb wichtig, die elektronische Signatur nahtlos in das bereits für die handschriftliche Unterschrift bestehende Rechtsgefüge einzupassen. Die elektronische Unterschrift muss neben der eigenhändigen Unterschrift als vollständig gleichwertige Unterschrift rechtlich anerkannt werden (diese Gleichstellung wird in Art. 1 Abs. 1 Bst. b ausdrücklich festgeschrieben). Es muss unseres Erachtens auf jeden Fall vermieden werden, durch entsprechende Wortwahl oder systematische Positionierung im Gesetz, die elektronische Unterschrift von der eigenhändigen abzuleiten bzw. sie als minderqualifizierte eigenhändige Unterschrift darzustellen. Vielmehr müssen die eigenhändige und die elektronische Unterschrift denselben rechtlichen Anerkennungsgrad erhalten, und beide Unterzeichnungsarten sind in eine gleiche Beziehung zum gemeinsamen Oberbegriff „Unterschrift“ zu setzen.

Der Unterschrift kommen vier grundsätzliche Funktionen zu: 1. Identifikation des Unterzeichneten; 2. zweifelsfreie Zuordnung der Unterschrift zum Unterzeichneten; 3. alleinige Verfügungsmacht des Unterzeichneten über die Unterschrift sowie 4. absolute Verknüpfung der Unterschrift mit dem unterzeichneten Dokument (Integrität). Neben diesen Formvorschriften kommt ein fünftes, materielles Element hinzu, nämlich die Absicht des Unterzeichneten, durch die Unterzeichnung eines Dokuments einen bestimmt gearteten Erklärungswillen abgeben und als seine Erklärung anerkennen zu wollen (Rekognition). Fehlt der Wille, das unterzeichnete Dokument als Erklärung des Unterschreibenden gelten zu lassen, liegt trotz Erfüllung der Form keine Unterschrift vor

(SCHÖNENBERGER Wilhelm, JÄGGI Peter, Kommentar zum Schweizerischen Zivilgesetzbuch 1973, Teilband V1a, Art. 13 N 20.).
Obwohl damit in formeller und materieller Hinsicht die Anforderungen an eine Unterschrift klar festgelegt sind, haben sich in der Praxis in den letzten Jahren eher pragmatische Lösungen durchgesetzt. Soweit den erwähnten materiellen Punkt der Rekognition betreffend (gemäss Punkt 5), muss diese nicht ausdrücklich erfolgen, sondern sie ergibt sich implizit aus der Stellung der Unterschrift unter das Dokument. Die elektronische Signatur erfüllt diese Anforderung, indem sie auf dem elektronisch signierten Dokument mittels Ausdruck effektiv und dauerhaft sichtbar gemacht werden kann. Durch die Verbindung mit dem Hash-Wert ist auch gewährleistet, dass die auf das Dokument bezogene Signatur erst nach der Erstellung des Textes gebildet werden kann. Was die Identifikation des Unterzeichneten betrifft (gemäss Punkt 1), ist Unterschrift zwar Namenszug (Art. 26 Handelsregisterverordnung [HRegV]), doch muss der Name nach bisheriger Praxis weder lesbar sein, noch unverkennbare Rückschlüsse auf die Person des Erklärenden zulassen(SCHÖNENBERGER, JÄGGI, Art. 14 und 15, N 9f.). Dies widerspricht zwar dem Sinn und Zweck des Gesetzes, doch darf diese Unsitte nicht dem nützen, der unleserlich unterschreibt. In dieser Hinsicht ist die elektronische Unterschrift dem ursprünglichen Sinn und Zweck der Norm wesentlich näher als die geltende Praxis zur handschriftlichen Unterschrift. Mittels digitaler Signatur, d.h. mittels privatem und öffentlichem Schlüssel, kann der Unterzeichnete eindeutig identifiziert und das unterzeichnete Dokument ihm zugeordnet werden. Diese Zuordnung wird in einem Signaturschlüssel-Zertifikat bescheinigt.
Auch betreffend der Verfügungsmacht (gemäss Punkt 3) ergeben sich keine wesentlichen Differenzen zwischen der handschriftlichen und der digitalen Signatur, ist doch in beiden Fällen grundsätzlich von der Verfügungsfähigkeit des Unterzeichneten über seine Unterschrift auszugehen, wobei sowohl im einen wie im anderen Fall Unterstellungen und Fälschungen möglich sind. Schliesslich sind auch die Anforderungen an die Integrität mehrseitiger Dokumente (gemäss Punkt 4) in der Praxis relativ lasch, werden doch üblicherweise einzelne Vertragsseiten nur an die die Unterschrift tragende Seite angeheftet (die Paraphierung jeder nicht unterzeichneten Seite erfolgt nur in Ausnahmefällen, insbesondere bei gesellschaftsrechtlichen Verträgen). Mittels digitaler Signatur kann demgegenüber die Einheitlichkeit des signierten Dokuments technisch gewährleistet werden, da die Signatur mit dem gesamten zu signierenden Datensatz über das mit der sogenannten Hashfunktion technisch erzeugten eindeutigen Dokumentenkomprimat logisch verknüpft ist.
Wie bereits erwähnt, ist bei der handschriftlichen und digitalen Unterschrift die inhaltliche und räumliche Abdeckung des Textes unter dem Erklärungstext gewährleistet, wobei unter gewissen Umständen auch heute ein besonderes Schriftstück zulässig ist (Allonge gemäss Art. 1003 OR). Schliesslich können auch elektronisch signierte Dokumente jederzeit optisch sichtbar gemacht und rechtsbeständig aufbewahrt werden.
Die rechtliche Gleichwertigkeit einer elektronischen Signatur gegenüber einer herkömmlichen Unterschrift wäre aufgrund dieser Ausführungen zu bejahen. Vergleicht man die geltende Praxis zur handschriftlichen Unterschrift mit den Anforderungen an eine digitale Signatur gemäss BG über die elektronische Signatur, so kann sogar festgestellt werden, dass die Letztere dem ursprünglichen Sinn und Zweck der Formvorschriften gemäss Art. 11 ff. OR wesentlich näher kommt als die heutige Praxis zur handschriftlichen Signatur.

Gemäss Wortlaut ist der Anwendungsbereich der elektronischen Signatur in doppelter Weise beschränkt, nämlich einerseits auf die Verträge und andererseits auf Verträge, die durch elektronischen Datenaustausch abgeschlossen werden (Art. 15a).
Wir gehen davon aus, dass trotz des Wortlauts von Art. 15a der Anwendungsbereich der digitalen Signatur nicht auf Verträge beschränkt werden soll und diese damit auch bei anderen Arten von Willensäusserungen eingesetzt werden kann. Wir verstehen, dass - aufgrund der fehlenden Rechtstradition und der Gesetzessystematik (Der erste Abschnitt des OR's regelt u.a. den Abschluss, die Form, die Auslegung, den Inhalt und die Abschlussmängel von Verträgen) - sich der E-BGES nicht auf die, eigentlich anvisierte, Willenserklärung beziehen kann. Wir sind jedoch der Ansicht, dass der Hinweis auf die Verträge nicht notwendig ist und ohne weiteres weggelassen werden kann. Sollte der Wortlaut trotzdem beibehalten werden, so würden wir es begrüssen, wenn in der Botschaft zum Gesetzesentwurf etwas stärker darauf hingewiesen würde, dass trotz Wortlaut andere Willensäusserungen (Dazu gehören nicht nur die weiteren Formen möglicher Willensäusserungen gemäss OR, sondern auch jene gemäss ZGB [Art. 7 ZGB]) von der Unterzeichnung mittels digitaler Signatur nicht ausgeschlossen sein sollen.
Im Zusammenhang mit der zweiten Einschränkung sind wir der Ansicht, dass diese nicht in den allgemeinen Teil des Obligationenrechts gehört. Soll die vertragliche Signatur tatsächlich auf elektronisch abgeschlossene Verträge beschränkt werden, was heissen würde, dass beide Parteien den Datenaustausch elektronisch abwickeln müssen, so sollte diese Einschränkung unseres Erachtens eher Bestandteil der Fernabsatz- oder E-Commerce-Gesetzgebung sein. Nach unserem Wissensstand kennen die Entwürfe der europäischen Staaten zur Implementierung der E-Signatur-Richtlinie keine entsprechenden Einschränkungen.
Die erwähnte Sach- und Rechtslage sollte unseres Erachtens sowohl gesetzessystematisch als auch sprachlich im revidierten OR reflektiert werden. Wir schlagen deshalb vor, die digitale Signatur unter der Marginale „c. Unterschrift“ und nicht nach der Marginale „d. Ersatz der Unterschrift“ zu regeln. Damit wäre die Gleichwertigkeit der handschriftlichen und digitalen Signatur auch gesetzessystematisch vollzogen (eine ähnliche Vorgehensweise ist auch in Artikel 1 des D-Entwurfs vorgesehen). Auf einer anderen Stufe steht demgegenüber Art. 15, der lediglich ein „Ersatz der Unterschrift“ und demzufolge nicht Unterschrift per se ist.
Wir schlagen deshalb vor, in einem Abs. 1 all jene Unterschriftsarten aufzuzählen, die der handschriftlichen gleichgestellt sind. Dazu gehören neben der elektronischen Unterschrift auch die Nachbildung einer eigenhändigen Unterschrift, wie dies bereits heute vor allem im Massenverkehr (Wertpapierrecht) der Fall ist. Damit wird auch der alternative Charakter der drei Unterzeichnungsarten herausgehoben. Demgegenüber würde die Unterschrift eines Blinden in einem separaten Abs. 2 verbleiben, da die Beglaubigung bzw. öffentliche Beurkundung sowohl für die eigenhändige Unterschrift als auch - sofern die hierfür notwendigen Strukturen geschaffen sind - für die elektronische Unterschrift Anwendung finden kann. Art. 15 OR würde dann auf Fälle Anwendung finden, da der Erklärende keine der drei Unterschriftsformen einsetzen kann, also auch die elektronische Signatur nicht.
Art. 14 *„[1]Als Unterschrift werden anerkannt:*
1. Die eigenhändige Unterschrift.

2. Eine Nachbildung der eigenhändigen Unterschrift auf mechanischem Wege, wo deren Gebrauch im Verkehr üblich ist, insbesondere wo es sich um die Unterschrift auf Wertpapieren handelt, die in grosser Zahl ausgegeben werden.
3. Die elektronische Signatur, wenn sie auf dem Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom °°° über die elektronische Signatur beruht.
[2]Für den Blinden ist die Unterschrift nur dann verbindlich, wenn sie beglaubigt ist oder wenn nachgewiesen wird, dass er zur Zeit der Unterzeichnung den Inhalt der Urkunde gekannt hat."

SAV Wie / Comme / Come Clusis.

Schlauri/Kohlas Der Vorentwurf sieht in einem neu einzufügenden Art. 15a OR für den Bereich der zivilrechtlichen Formvorschriften eine pauschale Gleichstellung von digitaler Signatur und Handunterschrift vor, sofern diese auf dem Zertifikat einer durch das BGES anerkannten Anbieterin von Zertifizierungsdiensten beruht. Eine derartige oder ähnliche Anerkennung ist u.E. eine Grundvoraussetzung für eine Verbreitung der digitalen Signatur und damit zu begrüssen.

Vor einer Gleichsetzung der digitalen Signatur mit der Handunterschrift bezüglich der Erfüllung gesetzlicher Formvorschriften ist jedoch zu prüfen, ob die digitale Signatur die jeweils in diesen Vorschriften relevanten Funktionen der Handunterschrift erfüllen kann. Denn der Begriff der digitalen Signatur ist die metaphorische Bezeichnung eines vergleichsweise komplexen technischen Instrumentes, das mit der traditionellen Handunterschrift nur wenig gemein hat. Dementsprechend kann vor übereilten Analogieschlüssen nur gewarnt werden.

Art. 15a OR sollte dahingehend lauten, dass die digitale Signatur der eigenhändigen Unterschrift dann gleichgestellt wird, wenn sie auf dem gültigen Zertifikat eines anerkannten Zertifizierungsdiensteanbieters beruht.

Die Funktionen der Handunterschrift sind primär die Beweisfunktion für Echtheit und Unveränderheit der Urkunde (diese spielt beispielsweise bei vielen miet- und pacht- und arbeitsrechtlichen Vorschriften oder zur Gewährung der Verkehrssicherheit bei der Zession eine Rolle) und die Warnfunktion (Übereilungsschutz bei Vertragstypen mit potentiell weitreichenden Folgen wie Schenkungsversprechen, Vorkaufsverträge über Grundstücke oder bestimmter Konsumentenverträge wie Ab- und Vorauszahlungsvertrag oder auch im Eherecht bei der Bestätigung des Scheidungswillens nach zweimonatiger Bedenkzeit). Gerade bezüglich der Warnfunktion sind digitale Signatur und Handunterschrift nicht äquivalent: Eine digitale Signatur kann – je nach Ausgestaltung des Signiersystems – mittels Eingabe eines Passwortes, mittels eines einfachen Mausklicks oder gar völlig automatisch gesetzt werden und entfaltet damit bedeutend weniger „Bremswirkung" (s etwa auch D. Gasser, Rechtsöffnung im Cyberspace?, AJP 1/2001, 91 ff., 93). Der Begleitbericht geht auf diese Problematik jedoch nicht ein und erwähnt nur lapidar, dass bei der Gleichsetzung von digitaler und Handunterschrift keine Ausnahmen gemacht würden.

Eine pauschale Anerkennung der digitalen Signatur ist aber abzulehnen, weil sie zu einer Aushöhlung der entsprechenden Schutzvorschriften führt (vl. auch D. Gasser, a.a.O.). Zwar gestaltet es sich teilweise schwierig, die Formvorschriften mit dominierender Warnfunktion von den übrigen abzugrenzen, dies sollte jedoch den Bemühungen des Gesetzgebers keinen Abbruch tun: Die einmalige klare Abgrenzung durch den Gesetzgeber verhindert Schwierigkeiten bei der Anwendung der Normen.

Widerrufsrecht für Konsumentenfernabsatzverträge als Abhilfe? Auch die Tatsache, dass eine ganze Reihe übereilungsgefährdeter Vertragstypen mit

dem durch den ebenfalls in der Vernehmlassung befindlichen Vorentwurf zu einem Bundesgesetz über den elektronischen Geschäftsverkehr vorgeschlagenen Widerrufsrecht für Konsumentenfernabsatzverträge entschärft werden sollen, spricht u.E. nicht für eine pauschale Anerkennung. Denn erstens kommt de lege lata der Übereilungsschutz der Handunterschrift in den Bereichen ausserhalb des Konsumentenschutzrechts (Schenkungsversprechen, Vorvertrag über Grundstückskauf, Bürgschaft) nicht nur dem Konsumenten, sondern jedem Vertragschliessenden zugute, zweitens deckt das genannte Widerrufsrecht für Fernabsatzverträge weite Bereiche nicht ab (Ausnahmen bestehen etwa für Finanzdienstleistungen und für nach genauen Angaben des Kunden angefertigte Güter), und drittens sollen die beiden Vorlagen zur elektronischen Unterschrift und zum elektronischen Geschäftsverkehr im Parlament getrennt behandelt werden, so dass bei einer Einführung der digitalen Signatur und Ablehnung des Widerrufsrechts weite Bereiche des Konsumentenschutzrechts in ihrer Funktion beeinträchtigt würden.

Dies macht – nebenbei bemerkt – deutlich, dass die von der Wirtschaft geforderte Aufteilung der beiden Vorlagen eigentlich alles andere als sinnvoll ist, weil bei einer Vorwegnahme der digitalen Signatur sämtliche Formvorschriften mit Übereilungsschutzzweck vorsorglich mit Ausnahmeklauseln versehen werden müssen, welche im Rahmen einer womöglich kurz darauf folgenden Annahme der neuen Fernabsatzregeln zumindest teilweise gleich wieder aufzuheben wären.

Einsatzgebiete der digitalen Signatur. Von einigen Seiten wird geltend gemacht, digitale Signaturen würden sich im privaten Bereich wohl vorderhand kaum durchsetzen, weil dem Konsumenten aus deren Einsatz primär Nachteile erwüchsen (vgl. etwa D. Rosenthal, Digitale Signaturen: Von Missverständnissen und gesetzlichen Tücken, Jusletter 29. Januar 2001, Rz 6). Daraus liesse sich schliessen, die Berücksichtigung des Übereilungsschutzes sei nicht prioritär. Auf die vorgeschlagenen Ausnahmeregelungen sollte jedoch u.E. nicht verzichtet werden, weil gerade ihr Fehlen auch zu noch mehr Zurückhaltung der Konsumentenschaft führen könnte, und weil auch bei einer nur mässigen Verbreitung das Bedürfnis nach Übereilungsschutz in diesen Einzelfällen bestehen bleibt.

Soll dieser Schutz bewusst nicht gewährleistet werden, müsste u.E. der digitalen Signatur die Anerkennung im nichtkaufmännischen Verkehr schlicht verwehrt werden.

Fazit : Diejenigen Formvorschriften, bei denen die digitale Signatur die Funktionen der Handunterschrift nicht oder nur ungenügend erfüllen kann, sollten also von der Regelung ausgenommen werden. Schliesslich entspräche dies auch der in der EU und in den USA vorgesehenen Lösung (Art. 9 der E-Commerce-Richtlinie; Section 103 des US-“Electronic Signatures in Global and National Commerce Act“; § 4 Abs. 2 des österreichischen Signaturgesetzes.).

Rosenthal Vgl. zu Art. 3 / Cf. ad art. 3 / Cfr. ad art. 3.

SBV Dans le domaine précontractuel notamment, il n'est pas rare que des dispositions légales requièrent la forme écrite. Les art. 13 à 15 CO s'appliquent par ailleurs à tous les actes juridiques et ne se limitent pas aux contrats. L'art. 15*a* CO, qui se réfère expressément aux contrats, est dès lors formulé de manière trop restrictive. Nous proposons donc de modifier cette disposition comme suit:

„Der eigenhändigen Unterschrift nach Artikel 14 gleichgestellt ist die elektronische Signatur, wenn sie auf dem Zertifikat einer anerkannten Anbieterin von

Zertifizierungsdiensten im Sinne des Bundesgesetzes vom xx über die elektronische Signatur beruht".
„La signature électronique est assimilée à la signature manuscrite au sens de l'article 14, lorsqu'elle repose sur un certificat d'un fournisseur de services de certification reconnu au sens de la loi fédérale du xx sur la signature électronique".

SUISA Ein Hauptpunkt der Vorlage ist die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift gemäss Art. 14 OR (Art. 15a E OR). Damit wird jedoch nur ein Grundsatz festgesetzt. Wie im Begleitbericht selbst festgehalten wird, ist es der Rechtsprechung überlassen, den Anwendungsbereich überall dort abzustecken, wo das Gesetz in irgend einer Art und Weise auf Schriftlichkeit verweist, ohne jedoch ausdrücklich die eigenhändige Unterschrift zu verlangen. Somit ist mit verbreiteter Rechtsunsicherheit zu rechnen. Diese scheint uns besonders hoch im Falle der provisorischen Rechtsöffnung nach Art. 82 SchKG, bei welcher die Praxis schon heute höchst disparat ist und zudem ein ordentliches Rechtsmittel ans Bundesgericht fehlt.

SVV Wie / Comme / Come SBV

SWICO Bei der Analyse des geänderten Artikels ist aufgefallen, dass sich der Entwurf nur auf den Vertragsabschluss bezieht. U.E. ist es an dieser Stelle notwendig, die Geltung auf sämtliche Willensäusserungen auszudehnen. Wir schlagen deshalb vor, den Artikel wie folgt zu ändern: „Der eigenhändigen Unterschrift nach Art. 14 gleichgestellt ist die elektronische Signatur, wenn sie auf dem Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom .... über die elektronische Signatur beruht."

TSM Das BGES und das BG über den elektronischen Geschäftsverkehr beziehen sich nur auf privatrechtliche Rechtshandlungen. Dieser Anwendungsbereich ist für die elektronische Signatur zu eng. Aus der Sicht der TSM ist es wichtig, dass die elektronische Unterschrift von Anfang an für alle möglichen Anwendungsbereiche juristisch geregelt wird. Neben den privatrechtlichen Rechtsgeschäften sollten darum auch alle Rechtshandlungen im öffentlichen Recht wie z.B. die Einreichung von Gesuchen nicht vergessen werden. Aus diesem Grund ist aus unserer Sicht eine Teilrevision nur eine provisorische und unvollständige Lösung. Vielmehr sollte die elektronische Signatur in einem selbständigen Gesetz (zumindest auf Bundesebene) geregelt werden. Dieser Erlass könnte dann alle Fragen im Zusammenhang mit der elektronischen Signatur regeln. Solche Fragen sind die Zertifizierung, der Anwendungsbereich (also auch Regelungen bezüglich aller anderer Rechtsgeschäfte als nur Verträge) und die Rechtsfolgen bei Missbrauch.

Dieser Erlass sollte die elektronische Signatur der eigenhändigen Unterschrift so weit als möglich gleichstellen und würde eine Teilrevision von OR und UWG zumindest ein Stück weit erübrigen.

Für die TSM ist es aus den oben genannten Gründen wichtig, dass der Gesetzgeber die elektronische Unterschrift generell der handschriftlichen Unterschrift gleichstellt. Die Signatur von elektronischen Rapportierungen soll sowohl in den Schutz des Privat- als auch des Strafrechts gelangen. Von grosser Bedeutung ist es für uns, dass die elektronische Signatur nicht nur im Bereich des Privatrechts, sondern auch im öffentlichen Recht als solche anerkannt wird. Es sollte die Möglichkeit geschaffen werden, alle Rechtshandlungen – von der Einreichung von Klagen und Rechtsmitteln bei Behörden bis zur Geltendmachung von Subventionen bei der TSM – auf dem elektronischen Weg geltend zu machen.

Vischer In das neue BGES eine generelle Bestimmung aufzunehmen, wonach die elektronische Signatur der eigenhändigen Unterschrift in allen vom Bundesrecht beherrschten Regelungsbereichen gleichgestellt ist. Der vorgeschlagene neue Art. 15a OR wird damit hinfällig.

Die systematische Einordnung dieser Bestimmung im Obligationenrecht bringt zum Ausdruck, dass diese Regelung sich auf den Begriff der eigenhändigen Unterschrift im Sinne von Art. 14 Abs. 1 OR und somit auf den zivilrechtlichen Schriftlichkeitsbegriff bezieht. Auf der Grundlage dieser Bestimmung sollen in Zukunft privatrechtliche Erklärungen, für welche das Gesetz die Schriftform als Gültigkeitsvoraussetzung vorsieht, in elektronischer Form verbindlich abgegeben werden können.

In diesem Zusammenhang ist jedoch daran zu erinnern, dass das schweizerische Recht nicht nur in Art. 12 ff. OR, sondern auch noch an anderen Orten auf die eigenhändige Unterschrift Bezug nimmt. Neben dem privatrechtlichen Begriff der Schriftlichkeit existieren noch andere gesetzliche Schriftlichkeitsbegriffe. Insbesondere zu erwähnen ist der betreibungsrechtliche Begriff der „durch Unterschrift bekräftigten Schuldanerkennung“, welcher gemäss Art. 82 SchKG den provisorischen Rechtsöffnungstitel charakterisiert. Der Begleitbericht zur Vernehmlassungsvorlage sagt dazu, dass der oben zitierte, neu vorgesehene Art. 15a OR dazu führen soll, „dass auch elektronisch signierte Schuldanerkennungen als provisorische Rechtsöffnungstitel gelten“ (Begleitbericht, S. 13). In der Gesetzesvorlage findet diese Aussage jedoch keine ausdrückliche Stütze. Es gibt auch noch weitere Gesetze, welche im einen oder anderen Zusammenhang auf die eigenhändige Unterschrift abstellen. So ist etwa in Art. 5 und Art. 178 des Bundesgesetzes über das Internationale Privatrecht eine vom bundesprivatrechtlichen Schriftlichkeitsbegriff abweichende „Textform“ als Gültigkeitsvoraussetzung für Gerichtsstands- und Schiedsabreden vorgesehen; solche Vereinbarungen können schriftlich, durch Telegramm, Telex, Telefax oder „in einer anderen Form der Übermittlung, die den Nachweis der Vereinbarung durch Text ermöglicht“, erfolgen. Auch das öffentliche Recht kennt schliesslich wiederum eigene Schriftlichkeitserfordernisse. Obwohl ausserhalb des Obligationenrechts vielfältige Gesetzesbestimmungen existieren, weiche in jeweils eigener Weise auf die eigenhändige Unterschrift Bezug nehmen, soll gemäss Vernehmlassungsvorlage nur im Obligationenrecht ausdrücklich auf die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift hingewiesen werden. Diese Lösung befriedigt nicht. Im Interesse der Klarheit und der Rechtssicherheit wäre zu wünschen, dass in das neue BGES eine generelle Bestimmung aufgenommen wird, wonach die elektronische Signatur der eigenhändigen Unterschrift in allen vom Bundesrecht beherrschten Regelungsbereichen gleichgestellt ist. Ein denkbarer Vorbehalt könnte lauten, dass diese Gleichstellung im Verkehr mit Behörden nur gilt, soweit eine Behörde sich zur Entgegennahme elektronisch signierter Erklärungen bereit erklärt hat oder die Entgegennahme solcher Erklärungen gesetzlich vorgesehen ist.

Erst mit der Aufnahme einer solchen generellen Bestimmung in das Spezialgesetz würde dieses neue Gesetz seinem in Art. 1 Abs. 2 lit. b normierten Zweck der „Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift“ gerecht werden. In der vorliegenden Entwurfsfassung erfüllt das neue Gesetz diesen Zweck nicht, weil gerade die Kernbestimmung über die rechtliche Qualität der elektronischen Signatur in das Obligationenrecht ausgelagert wurde.

VSG Alcuni ambiti toccati dalla revisione interessano l'attività dell'Ufficio del registro fondiario (forma scritta): cartelle ipotecarie (iscrizioni, modifiche, cancellazioni); servitù prediali in genere (passo, canalizzazione, ecc.); modifiche di fondi (frazionamenti, riunione, rettifica confini); successioni ereditarie; contratti di divisione ereditaria; annotazioni di diritti personali (locazione, prelazione semplice); esercizi diritti di compera/prelazione e ricupero; restrizioni della facoltà di disporre, pignoramenti e fallimenti.

Già oggi, in casi urgenti, le autorità e i tribunali possono richiedere per telefono o elettronicamente l'annotazione di una restrizione della facoltà di disporre e di un'iscrizione provvisoria (art. 13 cpv. 4 RFF): la richiesta è iscritta nel giornale con la data e il momento della comunicazione telefonica o elettronica (come accennato, nella comunicazione per via elettronica si pone infatti il problema del momento dell'effetto giuridico ex 972 CC).

Art. 15a CO (marginale: firma elettronica): se un contratto è concluso mediante scambio elettronico dei dati, la firma elettronica è equiparata alla firma autografa di cui all'art. 14 CO purché si fondi su un certificato di un prestatore di servizi di certificazione riconosciuto dalla legge federale sulla firma elettronica [LFiE]. Con l'introduzione del nuovo art. 15a CO si concretizza ulteriormente uno dei principi base del diritto contrattuale svizzero, ossia quello della libertà contrattuale. I contratti per i quali è prevista la forma scritta potranno essere conclusi anche per via elettronica: la firma elettronica sarà equiparata a quella autografa se si baserà su una coppia di chiavi certificata da un prestatore di servizi di certificazione riconosciuto dalla LFiE (pag. 4, 6 e 14 del rapporto esplicativo). Solo in questi casi subentra l'inversione dell'onere della prova ex art. 17 LFiE e la responsabilità del prestatore di servizi e del titolare della chiave privata (art. 17 e 18).

Le iscrizioni a registro fondiario avvengono (quasi) nella maggior parte dei casi sulla scorta di un atto pubblico (affidabilità di un documento; pag. 7). Con la firma e con il sistema di certificazione elettronica (chiavi) si potrebbe disporre di un procedimento che permette di determinare l'autenticità e l'integrità di un documento elettronico (pag. 9). Inoltre, la LFiE rappresenta la base legale per il riconoscimento e la responsabilità dei prestatori di servizio di certificazione (pag. 10).

In ogni caso, il principio che sottende all'intero progetto legislativo è quello di garantire l'autenticità e l'integrità dei documenti elettronici.

L'utilizzo della firma elettronica consente al mittente di un messaggio o documento elettronico di comprovare la propria identità, mentre il destinatario può verificare che dette comunicazioni non abbiano subito modifiche nel corso della trasmissione. Solo le firme digitali che rientrano nella LFiE garantiscono l'autenticità e l'integrità delle comunicazioni elettroniche poiché vengono certificate da parte di terzi affidabili, ossia i prestatori di sevizi di certificazione. Questi verificano l'identità del titolare di una chiave privata e confermano, in un certificato elettronico, l'appartenenza al titolare della chiave pubblica corrispondente.

Il progetto di legge non precisa il momento dal quale una dichiarazione di volontà debba essere ritenuta espressa e pervenuta (pag. 10 e 11). Questa mancata indicazione potrebbe rappresentare un problema per il momento dell'iscrizione a registro fondiario (indicazione a libro giornale).

La proposta di modifica dell'art. 15a CO non dovrebbe concernere i contratti per i quali è necessario l'atto pubblico e ribadisce l'autonomia a singoli Cantoni per determinare, sui loro territori, le norme per la celebrazione degli atti pubblici.

La nozione federale di atto pubblico non impedisce comunque ai Cantoni di prevedere che lo stesso sia redatto in forma elettronica e pertanto non è possibile escludere a priori tale eventualità, visto anche l'interesse già manifestato al riguardo da parte dei notai.
In effetti, come già ribadito, nonostante che, secondo quanto affermato dall'autorità federale, le iscrizioni nel registro fondiario e di commercio poggiano praticamente sempre su un atto pubblico (ma come visto ciò evidentemente non corrisponde alla realtà), è prevedibile che il privato cittadino probabilmente nei primi tempi non farà capo alla stesura di contratti in forma elettronica; saranno piuttosto i notai e gli istituti di credito a farne largo uso allorquando ciò sarà possibile.

VSW Anbieter von Gütern und Dienstleistungen im Internet haben tendenziell ein Interesse an elektronischen Signaturen, nicht zuletzt wohl auch deshalb, weil mit digitalen Signaturen versehene Bestellungen u.ä. Schuldanerkennungen im Sinne von Art. 82 SchKG darstellen, womit dem Anbieter im Verfahren der provisorischen Rechtsöffnung die einfache und rasche Vollstreckung von Geldforderungen ermöglicht wird.
Anders sieht die Situation auf der Seite der Konsumenten aus: Das auf dem Grundsatz der Formfreiheit (Art. 11 OR) beruhende schweizerische Vertragsrecht ermöglicht es den Konsumenten bereits heute, elektronische Verträge abzuschliessen. Auch sind dem gesetzlichen Formzwang unterliegenden Rechtsgeschäfte für elektronische B2C-Geschäftsmodelle kaum von Belang. Eine zwingende Notwendigkeit für sie, sich dem relativ umständlichen Verfahren der elektronischen Signatur zu unterziehen, gibt es deshalb kaum, zumal sie auch noch gewisse Haftungsrisiken eingehen müssen.
Ein weiteres kommt dazu: Das technische Problem ist nicht gelöst, wie elektronische Signaturen in die gebräuchlichen Online-Bestellformulare integriert werden könnten.

322.32 Art. 929a

Kantone / Cantons / Cantoni

AG Der Kanton Aargau führt sein Handelsregister schon seit Jahren in elektronischer Form. Insofern bringt der Abs. 1 dieser Bestimmung keine Veränderung. Diese neue Art der Registerführung hat sich bestens bewährt.
Eine wesentliche Neuerung bringt Abs. 2 (elektronische Einreichung von Anmeldungen beim Handelsregister). Obwohl, wie im Begleitbericht unter Ziff. 231 f. zutreffend ausgeführt, die elektronische Anmeldung zur Zeit noch nicht realisierbar ist, darf nicht auf diese zukunftsorientierte Gesetzesnorm verzichtet werden. In diesem Bereich ist ein gesamtschweizerisches Vorgehen unerlässlich. Ziel muss es sein, den Verbund der kantonalen Handelsregister so zu intensivieren, dass der Kunde über eine gemeinsame Plattform auf dem Internet einsteigen kann und dann zu demjenigen Handelsregister gelangt, das für seinen Eintrag zuständig ist.
Der elektronisch signierte Handelsregisterauszug wäre eine von den Kunden sehr gewünschte Erweiterung des Angebots, insbesondere im internationalen Verkehr. Dass der Bund in Art. 929a Abs. 2 OR die Kompetenz erhalten soll, den Kantonen die Erstellung solcher Auszüge vorzuschreiben, ist konsequent, denn der Wirtschaftsraum Schweiz ist nur dann international attraktiv, wenn er von aussen als Einheit wahrgenommen wird. Dies setzt einheitliche Standards bei allen Kantonen voraus.

BL Im Bereich des Handelsregisters begrüssen wir, dass dem Bundesrat ermöglicht werden soll, die Akzeptanz elektronischer Anmeldungen und Belege sowie das Ausstellen von beglaubigten, elektronisch signierten Handelsregisterauszügen einheitlich zu regeln (Art. 929a Abs. 1 und 2 VE OR). Dadurch werden den Rechtsverkehr hemmende, kantonal unterschiedliche Praktiken und Systemlösungen vermieden.

BS Ist der Empfang elektronisch signierter Anmeldungen und Belege noch einigermassen unproblematisch und ist in diesem Zusammenhang einfach sicherzustellen, dass die auf diese Weise eingereichten Belege Eingang in die Geschäftskontrolle und in den Arbeitsablauf des Handelsregisteramtes finden, stellen sich im Zusammenhang mit der Aufbewahrung dieser Belege zahlreiche Fragen.

Die sichere Archivierung elektronisch zugestellter Anmeldungen und Belege muss über mehrere Jahre und Jahrzehnte gewährleistet sein. Die Beleg-Dateien müssen in allgemein gängigen Formaten abgelegt und zwischen den Handelsregisterämtern beliebig austauschbar sein. Die Daten müssen jederzeit - auch noch nach mehreren Jahren und Jahrzehnten - lesbar und verfügbar sein.

Im Zusammenhang der Sitzverlegung von im Handelsregister eingetragenen Rechtsträgern ergeben sich insofern Probleme, als ein Rechtsträger seinen Sitz in einen Registerbezirk verlegt, der im Zeitpunkt der Sitzverlegung noch nicht in der Lage ist, digital signierte Anmeldungen und Belege entgegenzunehmen. Deshalb wären alle Handelsregisterämter in der Schweiz zur Entgegennahme von digital signierten Anmeldungen und Belegen unabhängig davon zu verpflichten, ob die Handelsregisterführung bereits mit den Mitteln der elektronischen Datenverarbeitung erfolgt oder nicht. Jeder Kanton wäre demzufolge zu verpflichten, entsprechend digital signierte Anmeldungen und Belege entgegenzunehmen.

Diese Lösung hätte auch insofern positive Auswirkungen, als alle Kantone gezwungen wären, möglichst rasch die erforderlichen Regelungen zu treffen, um eine geregelte Handhabung des Empfangs von elektronisch signierten Anmeldungen und Belegen zu gewährleisten. Selbst ohne solche Regelungen wären die Kantone nämlich gleichwohl verpflichtet, entsprechende Belege aus anderen Kantonen, insbesondere aber auch aus dem Ausland (HRegV Art. 30), entgegenzunehmen und zur Eintragung zu bringen.

Um eine rasche Einführung zu gewährleisten, scheint es sinnvoll eine Übergangslösung zu treffen, welche den einzelnen kantonalen Handelsregisterämtern eine sichere Aufbewahrung der elektronisch eingereichten Belege ermöglicht, ohne dass alle kantonalen Handelsregisterämter bereits über eine volle Archivlösung verfügen müssten.

Im Zusammenhang mit der Einreichung von digital signierten Anmeldungen und Belegen beim zuständigen Handelsregisteramt ergibt sich das Problem, dass nicht nur solche Belege eingereicht werden, welche mit Signaturen schweizerischer Zertifizierungsstellen versehen sind. Vielmehr werden die Handelsregisterämter (und auch die übrigen Behörden) mit elektronischen Zertifikaten konfrontiert werden, welche von Zertifizierungsstellen im Ausland ausgestellt worden sind. Hier wird darauf zu achten sein, dass die Zertifikate oder die digitalen Signaturen von Zertifizierungsstellen ausgestellt worden sind, welche an die Überprüfung der Identität der Zertifikatsinhaber hohe und höchste Anforderungen stellen. Nur auf diese Weise kann gewährleistet werden, dass die einzureichenden Anmeldungen als höchstpersönliche und unübertragbare Erklä-

rungen, sowie auch die einzureichenden Belege tatsächlich von den aus den Zertifikaten hervorgehenden Zertifikats-Inhabern stammen. Eine persönliche Überprüfung der Identität des Zertifikatsinhabers durch die Zertifizierungsstelle oder durch eine ihr zugeordnete Registrierungsstelle wird demzufolge für die Einreichung eines digital signierten Belegs oder einer digital signierten Anmeldung unabdingbare Bedingung sein müssen.
Die von der derzeit in der Schweiz einzigen Zertifizierungsstelle ausgestellten Zertifikate haben eine Gültigkeitsdauer von zwei Jahren. Verschiedene Anwender fordern eine Verlängerung dieser Gültigkeitsdauer auf drei Jahre. Nach Ablauf der Gültigkeitsdauer eines Zertifikates ist die Zertifizierungsstelle verpflichtet, den öffentlichen Schlüssel eines Zertifikates zur Überprüfung entsprechend signierter Dokumente noch während eines Zeitraumes von zehn Jahren auf einem allgemein zugänglichen Server gebührenpflichtig zur Verfügung zu halten. Handelsregisterämter müssen digital signierte Anmeldungen und Belege über einen Zeitraum von wesentlich mehr als zehn Jahren in ihren Archiven aufbewahren. Es ist deshalb unabdingbar, dass die entsprechenden öffentlichen Schlüssel der Zertifikate ebenfalls über einen wesentlich längeren Zeitraum als zehn Jahre aufbewahrt und verfügbar gemacht werden können. Es ist demzufolge unumgänglich, dass die Handelsregisterämter im Moment der Einreichung einer digital signierten Anmeldung oder eines digital signierten Belegs die öffentlichen Schlüssel der Zertifikate, die selbstverständlich im Moment der Einreichung eines Belegs oder einer Anmeldung noch gültig sein müssen, so aufbewahrt - d.h. speichert -, dass eine Überprüfung digital signierter Anmeldungen und Belege auch noch mehrere Jahre, ja sogar Jahrzehnte nach der Einreichung solcher Belege möglich ist.
Für die Frage, ob der Erlass von digital signierten Verfügungen durch das Handelsregisteramt zulässig sein soll, kann auf die Ausführungen bezüglich der Ausstellung von digital signierten Handelsregisterauszügen verwiesen werden. Ohne vorliegend auf die Einzelheiten der Problematik einzutreten, sei immerhin angemerkt, dass der Erlass von digital signierten Verfügungen insbesondere dann völlig unproblematisch erscheint, wenn auch die zum Erlass der Verfügung führenden Anträge in elektronischer und digital signierter Form der zuständigen Behörde eingereicht worden sind.
Elektronische Führung des Handelsregisters (*E-OR* Art. 929a Abs. I): Die elektronische Führung des Handelsregisters ist keine Novität. Die überwiegende Mehrheit der Kantone führt das Handelsregister bereits heute auf elektronischer Basis. Die Kantone haben aus eigener Initiative entsprechende Entwicklungen gemacht und auch finanziert. Die vorliegend vorgeschlagene Regelung visiert somit lediglich diejenigen wenigen Kantone an, welche sich bisher erfolgreich einer Realisierung der elektronischen Führung des Handelsregisters entzogen haben. Auch diese Kantone sollen nun endlich zur Einführung der elektronischen Registerführung verpflichtet werden.
Aus unserer Sicht scheint es selbstverständlich sinnvoll, alle Kantone zur elektronischen Führung des Handelsregisters zu verpflichten. Es ist ausserordentlich schade, dass das Ziel einer flächendeckenden elektronischen Handelsregisterführung in der Schweiz nicht bereits heute erreicht ist. Der Bund setzt hier entsprechend dem Sprichwort „mieux vaut tard que jamais“ die erforderlichen Signale. Dabei kann man sich immerhin fragen, ob das Problem für die wenigen, betroffenen Kantone wirklich noch einer expliziten Regelung lohnt, oder ob die betroffenen Kantone nicht auf anderem Wege „überzeugt“ werden könnten.

Im Hinblick auf die vorliegend zu prüfenden Fragen der elektronischen Zertifikate und digitalen Signaturen gilt es festzuhalten, dass zwischen der elektronischen Führung des Handelsregisters und den elektronischen Zertifikaten oder den digitalen Signaturen, als derzeit wohl wichtigstem Anwendungsfall elektronischer Signaturen, nur ein mittelbarer Zusammenhang besteht. Der Zusammenhang ist insofern gegeben, als die Verwendung elektronischer Zertifikate und digitaler Signaturen für ein einzelnes Handelsregisteramt dann kaum Sinn macht, wenn die Handelsregisterdaten noch nicht elektronisch erfasst sind. Über diesen bloss mittelbaren Zusammenhang hinaus bestehen allerdings keine weiteren Zusammenhänge zwischen elektronischer Registerführung und digitalen Zertifikaten oder digitalen Signaturen. Man kann sich somit den „Vorwurf“ kaum ersparen, dass die Einführung der Verwendung von digitalen Signaturen gleichzeitig zur Einführung einer Pflicht zur elektronischen Registerführung „missbraucht“ werden soll.

Aller Kritik zum Trotz scheint es im Ergebnis gleichwohl angezeigt, die elektronische Führung des Handelsregisters nunmehr explizit zu statuieren. Dies, wenn man davon ausgeht, dass die Durchsetzung einer an sich selbstverständlichen elektronischen Führung des Handelsregisters einer gesetzlichen Grundlage zumindest in Form einer Delegationsnorm bedarf.

Elektronischer Datenaustausch zwischen den Handelsregisterbehörden (E-OR Art. 929a Abs. I): Was zur Frage der elektronischen Führung des Handelsregisters bereits ausgeführt wurde, gilt in verstärktem Masse für den elektronischen Datenaustausch zwischen den Handelsregisterbehörden. Entsprechend der „Weisung über die elektronische Übermittlung des HR-Tagebuches (Art. 114 Abs. 1 HRegV) und über die Anwendungsvoraussetzungen des Art. 23 Abs. 2 Geb'Tarifs“ des Eidgenössischen Amtes für das Handelsregister vom 15. August 1995 sind die Grundvoraussetzungen für eine elektronische Übermittlung der Handelsregisterdaten zwischen Bund und Kantonen bereits seit längerer Zeit gegeben. Auch hier geht es darum, die Handelsregisterämter von der Notwendigkeit zu überzeugen, ihre Handelsregisterdaten elektronisch zu übermitteln. Der Datenaustausch zwischen den Kantonen ist übrigens ebenfalls bereits heute realisiert und wurde im Zusammenhang mit dem Aufbau der Internet-Auftritte durch die auf dem Internet präsenten Kantone - derzeit immerhin 16 Kantone - verwirklicht. Diese Formen des Datenaustauschs sind bereits seit längerer Zeit standardisiert (UN-EDIFACT-Meldung gemäss der bereits zitierten Weisung vom 25. August 1995) und in ein entsprechendes Regelwerk gefasst. Immerhin sei angemerkt, dass hier eine Ablösung der Übermittlungsstandards in Vorbereitung ist und im Verlaufe des nächsten Jahres in Angriff genommen wird. Die Übertragung der Daten wird meldungsbasiert neu nach dem heute gängigen XML-Standard erfolgen.

Beachtenswert ist im gegebenen Zusammenhang immerhin, dass der elektronische Datenaustausch zwischen den Handelsregisterbehörden im Grunde gar nichts mit den Fragen der digitalen Signatur als Anwendungsfall elektronischer Zertifikate zu tun hat. Im Gegensatz zur elektronischen Führung des Handelsregisters fehlt es hier sogar an einem mittelbaren Zusammenhang. Dies mit dem kleinen Vorbehalt, dass man die - heute geschützt und verschlüsselt - ausgetauschten Daten allenfalls auch noch digital signieren könnte. Aus einer Möglichkeit kann eine Pflicht entstehen.

Aller Kritik zum Trotz scheint es im Ergebnis allerdings auch hier angezeigt, die elektronische Datenübermittlung zwischen den Handelsregisterbehörden der Kantone einerseits und zwischen den kantonalen Handelsregisterbehörden und

dem Eidgenössischen Amt für das Handelsregister (EHRA) andererseits nunmehr explizit zu statuieren. Dies, um zu gewährleisten, dass endlich ein elektronischer Datenaustausch für alle Handelsregisterämter in der Schweiz realisiert werden kann.
Nachdem die bisher behandelten Fragen der elektronischen Führung des Handelsregisters und des elektronischen Datenaustausches zwischen den Handelsregisterbehörden in höchstens mittelbarem Zusammenhang mit digitalen Signaturen und elektronischen Zertifikaten stehen, stellen die beiden nachfolgend zu behandelnden Problemkreise direkte Anwendungsfälle elektronischer Zertifikate und digitaler Signaturen dar. Es sei zunächst die Möglichkeit der Statuierung einer Pflicht zur Ausstellung digital signierter Handelsregisterauszüge behandelt :
Pflicht zur Ausstellung von beglaubigten, digital signierten Handelsregisterauszügen (E-OR Art. 929a Abs. II Satz 2): Handelsregisterauszüge werden heute einerseits in Papierform und andererseits - zumindest von sechzehn Kantonen - online via Internet angeboten. Die auf Papier bezogenen Handelsregisterauszüge sind regelmässig beglaubigt. Nur ein Teil der kantonalen Handelsregisterämter - nicht so das Handelsregisteramt des Kantons Basel-Stadt - stellt Handelsregisterauszüge auf Papier auch in unbeglaubigter Form aus.
Sechzehn Kantone - das heisst bereits eine Mehrheit der Kantone, insbesondere was die Zahl der eingetragenen Rechtsträger betrifft - stellen Handelsregisterauszüge auch via Internet zur Verfügung. Mangels entsprechender gesetzlicher Grundlage, können diese Handelsregisterauszüge bisher nur in unbeglaubigter Form bezogen werden. Entsprechend den Bedürfnissen der Wirtschaft ist es dringend geboten, dass Handelsregisterauszüge online auch in beglaubigter Form bezogen werden können. Zu diesem Zweck müssen online bezogene Handelsregisterauszüge digital signiert werden können. Die vorgeschlagene Regelung sieht vor, dass der Bundesrat «den Kantonen die Ausstellung beglaubigter, digital signierter Handelsregisterauszüge vorschreiben kann». Derzeit sind die technischen Möglichkeiten für die Ausstellung von digital signierten Handelsregisterauszügen bereits vollumfänglich gegeben. Diejenigen Kantone, welche bereits heute via Internet unbeglaubigte Handelsregisterauszüge ausstellen, haben neben dem Erwerb eines entsprechenden, das digitale Signieren von Handelsregisterauszügen ermöglichenden Zertifikates sowie allfälligen Anpassungen der Handelsregister-Software keinerlei zusätzliche Investitionen zu tätigen. Aus diesem Grunde sollte die Möglichkeit des Ausstellens digital signierter Handelsregisterauszüge so rasch wie möglich in die Praxis umgesetzt werden. Der Wortlaut der vorgeschlagenen Regelung lässt es den Kantonen zumindest bezüglich der Ausstellung von beglaubigten Handelsregisterauszügen offen, solche Auszüge auch ohne entsprechende Vorschrift des Bundesrechts (Verordnung des Bundesrates) auszustellen. Dies gilt jedenfalls ab dem Moment, wo die eigenhändige Unterschrift der digitalen Signatur gleichgestellt sein wird.
Entsprechend den steigenden Bedürfnissen der Wirtschaft auf nationaler und internationaler Ebene ist bereits ein Zeitraum von einem Tag zwischen Bestellung und Eintreffen des Handelsregisterauszuges zu lang. Die entsprechenden Informationen aus dem Handelsregister müssen sofort, das heisst innert weniger Minuten zur Verfügung stehen, wenn die Handelsregisterinformationen ihren Zweck auch in Zukunft erfüllen sollen und nicht durch entsprechende Angebote der Privatwirtschaft zumindest faktisch abgelöst werden wollen.
Wenn das Handelsregister in der Schweiz seine Bedeutung als wesentliches Mittel zur Gewährleistung eines sicheren und transparenten Rechtsverkehrs

behalten will, ist die Möglichkeit zur Online-Ausstellung von beglaubigten Handelsregisterauszügen unabdingbar. Der Bedeutung dieser Möglichkeit für den „Wirtschaftsstandort Schweiz“ ist in diesem Zusammenhang besondere Beachtung zu schenken.
Damit sind alle möglichen Anstrengungen zu unternehmen, damit möglichst rasch online beglaubigte Handelsregisterauszüge ausgestellt werden können. Es ist in jedem Falle darauf zu achten, dass mit der Ausstellung von beglaubigten Handelsregisterauszügen seitens der Kantone stufenweise begonnen werden kann. Es ist demzufolge beispielsweise nicht zuzuwarten, bis auch der letzte Kanton in der Lage ist, Handelsregisterauszüge online auszustellen. Vielmehr sollen die einzelnen Kantone entsprechend ihren Möglichkeiten mit der Online-Ausstellung von beglaubigten Handelsregisterauszügen beginnen können.
Zulässigkeit und Voraussetzungen zur elektronischen Einreichung digital signierter Anmeldungen und Belege beim Handelsregisteramt (E-OR Art. 929a Abs. II Satz 1).
Gemäss dem vorgeschlagenen E-OR Art. 929a Abs. II Satz 1 bestimmt der Bundesrat, „ob und unter welchen Voraussetzungen die elektronische Einreichung digital signierter Anmeldungen und Belege beim Handelsregister zulässig ist.“
Bevor auf die Einzelheiten einzugehen sein wird, sind im Zusammenhang mit der vorgeschlagenen Regelung zwei grundsätzliche Punkte festzuhalten:
Die vorgeschlagene Regelung beinhaltet einen Vorbehalt zugunsten des Bundes. Soweit und solange der Bundesrat keine entsprechende Regelung getroffen hat, bleibt es den Kantonen - anders als bei der Regelung für die Ausstellung beglaubigter digital signierter Handelsregisterauszüge - damit explizit verwehrt, für die elektronische Einreichung digital signierter Anmeldungen und Belege eine Regelung zu treffen und damit die Einreichung digital signierter Anmeldungen und Belege zu ermöglichen.
Diese Lösung erstaunt insofern, als bisher bei allen technischen Entwicklungen die Kantone lange vor entsprechendem Reagieren des Bundes vorangeschritten sind und Lösungen entwickelt und finanziert haben, die sich heute in der Praxis bewährt haben und bewähren. Warum durch die vorgeschlagene Lösung der Aktionsradius der Kantone durch eine ausschliessliche Kompetenz des Bundes blockiert werden soll, erscheint unklar. Auf diese Weise wird das Vorantreiben technischer Entwicklungen in diesem Bereich in einer Weise behindert, die - entsprechend den bisherigen Erfahrungen - für das gesamte System schädlich sein kann. Demzufolge erscheint eine Regelung im Rahmen einer parallelen Kompetenz von Bund und Kantonen, welche dem Bund die Aufgabe überträgt, die erforderlichen Rahmenbedingungen für die elektronische Einreichung digital signierter Anmeldungen und Belege festzulegen und die interkantonale Koordination zu regeln, wesentlich sinnvoller. Auf diese Weise wäre die Koordinationsfunktion des Bundes in diesem Bereich sichergestellt und die Kantone in ihren Entwicklungen nicht behindert.
Der Wortlaut von E-OR Art. 929a Abs. II Satz 1 ist insofern zu ergänzen, als die Einreichung der elektronisch signierten Anmeldungen und Belege nicht beim „Handelsregister“, sondern beim „Handelsregisteramt“ erfolgt. Das Handelsregister ist entsprechend der massgeblichen Definition das Register, in das die Daten eingetragen werden. Das Handelsregisteramt ist die Behörde, welche für die Vornahme solcher Eintragungen zuständig ist.

Nach diesen beiden einleitenden, eher formellen Aspekten, ist nun auf die materiellen Aspekte der Einreichung von digital signierten Anmeldungen und Belegen beim Handelsregisteramt einzugehen :
Rolle der Urkundspersonen: Im Zusammenhang mit der Einreichung von digital signierten Anmeldungen und Belegen beim Handelsregisteramt - aber auch bei anderen Behörden (z.B. Grundbuchämtern, Gerichten etc.) wird im Zusammenhang mit der öffentlichen Beurkundung von solchen Dokumenten immer wieder Widerstand - wenn nicht sogar Unverständnis - von den für die Verurkundung zuständigen Urkundspersonen laut.
Es sei an dieser Stelle festgehalten, dass die entsprechend den jeweils massgeblichen kantonalen Bestimmungen zuständigen Urkundspersonen oder Organisationen (Notarinnen und Notare, Amtsnotariate, Bezirksschreibereien, Gemeinden etc.) durch die Einführung von digital signierten Anmeldungen und Belegen in der Erfüllung ihrer Aufgabe in keiner Art und Weise beeinträchtigt oder gar beschnitten werden. Der Unterschied liegt lediglich darin, dass die im Rahmen der Durchführung einer Verurkundung ausgefertigten Belege nicht mehr in Form von Papier, sondern neu in Form von digital signierten Dateien dem Handelsregisteramt (oder anderen Behörden) einzureichen sind.
Es werden wohl regelmässig Änderungen des jeweiligen kantonalen Notariatsrechts erforderlich sein, um die Rahmenbedingungen für digital signierte elektronische öffentliche Urkunden zu schaffen. Doch ändert dies beispielsweise nichts an der Tatsache, dass die Parteien oder deren Vertreter persönlich vor dem Notar zur Verurkundung der rechtserheblichen Tatsachen entsprechend dem aktuellen Verständnis des Begriffs der öffentlichen Urkunde erscheinen müssen.
Allein die vorliegenden Ausführungen machen deutlich, dass die Urkundspersonen bei der Frage der Zulässigkeit von digital signierten Anmeldungen und Belegen keine entscheidende Rolle spielen. Sie sind als Intermediär zwischen Kundinnen und Kunden und registerführenden Behörden lediglich für die Verurkundung sowie für die Beratung der Kundinnen und Kunden zuständig und verantwortlich. In welcher Form sie Urkunden aufbereiten und den zuständigen Behörden einreichen, ist für die Ausübung der Tätigkeit der Urkundspersonen nicht von übergeordneter Bedeutung.
Da anlässlich einer Verurkundung beispielsweise der Gründung einer Aktiengesellschaft heute regelmässig den Gründern die Unterlagen in Papierform vorgelegt werden, wird es Sache der Urkundsperson sein, im Anschluss an die Verurkundung von den Belegen mehrere Ausfertigungen der notariellen Urkunden zu erstellen. Dabei sollte er die Möglichkeit haben, solche Ausfertigungen auch in elektronischer Form digital signiert zu erstellen, um diese schliesslich den zuständigen Behörden - beispielsweise also dem Handelsregisteramt - einzureichen.
Der vorliegende Entwurf könnte den Verdacht aufkommen lassen, dass der Bundesrat auch eine Regelung vorsehen könnte, welche die Einreichung von digital signierten Anmeldungen und Belegen vollständig ausschliesst. Anders ist doch wohl die Verwendung der Konjunktion „ob“ kaum zu deuten. An dieser Stelle sei deshalb betont, dass eine Regelung, welche die Einreichung von digital signierten Anmeldungen und Belegen ausschliesst, schlicht undenkbar ist. Ein kurzer Blick auf die internationale Rechtsentwicklung vermag diese Feststellung zu bestätigen.
Am 1. Januar 2000 ist in Österreich das Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG) in Kraft getreten (BGBl I 1990/190). Bereits

heute - nur 15 Monate nach dem Inkrafttreten des Signaturgesetzes - können die dem Firmenbuch (= Handelsregisteramt in Österreich) einzureichenden Jahresabschlüsse auf elektronischem Wege digital signiert eingereicht werden.
Auch bei den italienischen Handelsregisterbehörden (INFOCAMERE) können gestützt auf das Gesetz No 59 vom 15. März 1997 [Gazzetta Ufficiale no 63 vom 17. März 1997) bereits heute elektronische Belege eingereicht werden. Die italienischen Handelsregisterämter (INFOCAMERE) reden sogar explizit davon, dass die Belege ausschliesslich in elektronischer Form eingereicht werden sollen. Gleichzeitig treten die italienischen Handelsregisterämter als Zertifizierungsstellen (nicht bloss als Registrierungsstellen!) für elektronische Signaturen auf. In diesem Zusammenhang vergeben sie anlässlich der Eintragung einer Gesellschaft sogenannte Smartcards, welche das elektronische Zertifikat enthalten. Andere Formen elektronischer Zertifikate oder elektronischer Signaturen werden - zumindest derzeit - nicht ausgegeben.
Frankreich hat seine entsprechende Gesetzgebung am 13. März 2000 angenommen (Acte no 2000-230 vom 13. März 2000) und ist nun im Bereiche der Handelsregisterämter ebenfalls dabei, eine Lösung vorzubereiten.
Companies House in Grossbritannien (Cardiff [GB]) bereitet eine Lösung vor, welche die Einreichung von Anmeldungen via Internet ermöglichen soll. Diese Lösung entspricht im übrigen einer Lösung, welche derzeit von den Handelsregisterämtern der Kantone Zürich und Basel-Stadt vorbereitet wird. Solange digitale Signaturen nicht zugelassen sind, ist jeweils nach der Erfassung der Daten durch die Kundinnen und Kunden ein Exemplar der Anmeldung auszudrucken, zu unterzeichnen und zusammen mit den übrigen Belegen in Papierform dem zuständigen Handelsregisteramt zur Eintragung einzureichen. Dies gilt übrigens sowohl für Companies House in Grossbritannien als auch für die erwähnten Handelsregisterämter in der Schweiz.
Verschiedene andere Staaten haben bereits entsprechende Signaturgesetze verabschiedet und sind derzeit in Vorbereitung ähnlicher Lösungen.
Der kurze internationale Überblick zeigt, dass für die Schweiz im Interesse des Wirtschaftsstandortes auch in diesem Bereich dringender Handlungsbedarf besteht.
Im Gegensatz zur Ausstellung von digital signierten Handelsregisterauszügen, ergeben sich im Zusammenhang mit der Einreichung von digital signierten Anmeldungen und Belegen insbesondere für die kantonalen Handelsregisterämter zahlreiche offene Fragen und Probleme, die es zu lösen gilt.
Erwähnt seien hier beispielsweise die Frage der Archivierung der Belege, die Problematik, ob und inwieweit die Belege parallel auch auf Papier einzureichen sind oder ob das zuständige Handelsregisteramt zumindest die elektronisch eingereichten Belege auszudrucken und zu archivieren hat.
Die Klärung dieser und weiterer Fragen ist nun möglichst rasch an die Hand zu nehmen und sollte in den Grundzügen, das heisst insofern Dritte davon betroffen sind, Gegenstand der bundesrätlichen Verordnung bilden. Dritte nicht betreffende Einzelheiten der Regelung müssten Gegenstand einer Weisung des Eidgenössischen Amtes für das Handelsregister an die kantonalen Handelsregisterbehörden bilden.
Die vorgeschlagene Lösung einer bundesrätlichen Verordnung hat den wesentlichen Vorteil, dass auch nach dem Erlass der Verordnung, im Hinblick auf die raschen technischen Veränderungen in diesem Bereich, eine im Vergleich zu einer Regelung auf Gesetzesstufe verhältnismässig unkomplizierte und schnelle Anpassung möglich ist. Von besonderer Bedeutung aber ist, dass die

dem Bundesrat eingeräumte Kompetenz nicht einfach toter Buchstabe bleibt, sondern so rasch wie möglich die Arbeiten für den Erlass einer entsprechenden Verordnung sowie einer zugehörigen Weisung des Eidgenössischen Amtes für das Handelsregister an die Hand genommen werden. Nur so ist es möglich, innert nützlicher Frist die erforderlichen Regelungen vorzubereiten und in Kraft treten zu lassen.

Wie bereits erwähnt, erscheint insbesondere die Tatsache von Nachteil, dass die Kompetenz des Bundesrates im Bereiche der Einreichung von digital signierten Anmeldungen und Belegen eine ausschliessliche sein soll. Den Kantonen bleibt es demzufolge bis zum Erlass einer entsprechenden Verordnung des Bundesrates verwehrt, selbständige Regelungen in diesem Bereiche zu treffen. Auch aus diesem Grunde ist demzufolge rasches Handeln geboten. Es sei an dieser Stelle noch einmal betont, dass aus unserer Sicht in diesem Bereich eine parallele Kompetenz von Bund und Kantonen der vorgeschlagenen Regelung vorzuziehen wäre.

Unter der Voraussetzung aber, dass die vorgeschlagene Regelung rasch in Kraft tritt und die zugehörige Verordnung des Bundesrates sowie die wohl erforderliche Weisung des Eidgenössischen Amtes für das Handelsregister nach entsprechender Vorbereitung ebenfalls sehr bald in Kraft gesetzt werden können, erscheint der vorgeschlagene Entwurf durchaus tragbar.

Die vorliegend zu beurteilende Einführung von digital signierten Anmeldungen und Belegen, aber auch von digital signierten Handelsregisterauszügen, wird für die Erfüllung der Aufgaben eines Handelsregisteramtes von höchster Priorität sein. Wenn die Handelsregisterämter den Bedürfnissen der Wirtschaft nach raschen und klaren sowie korrekten Informationen nicht mehr gerecht werden, wird die Bedeutung der Handelsregisterämter deshalb an Gewicht verlieren, weil sie nicht mehr in der Lage sein werden, innerhalb der geforderten Zeit der Wirtschaft die für einen geordneten und sicheren Rechtsverkehr erforderlichen Informationen zu liefern. Man darf deshalb - trotz aller übrigen bedeutungsvollen Revisionsvorhaben beispielsweise im Bereiche des GmbH-Rechts und des Fusionsgesetzes - die Bedeutung dieser Revision für die Zukunft des Handelsregisterwesens keinesfalls unterschätzen.

Erfüllen die staatlichen Behörden die ihnen in diesem Bereiche obliegenden Aufgaben nicht oder nur unvollständig, werden diese zumindest mittelfristig durch private Organisationen abgelöst werden, welche für die Gewährleistung eines geordneten und sicheren Rechtsverkehrs mit den neuen technischen Möglichkeiten entsprechend den Bedürfnissen der Wirtschaft Gewähr zu bieten in der Lage sind.

GR Die neu vorgeschlagenen Art. 929a und 931 Abs. 2^{bis} OR bilden lediglich eine vage Grundlage für die Einführung des digitalen Verhaltens im Handelsregisterwesen. Es werden verschiedene noch nicht konkretisierte Vorgehensweisen der elektronischen Führung des Handelsregisters angesprochen. Der Ausgestaltung in den noch zu erlassenden Ausführungsvorschriften des Bundesrates wird deshalb eine grosse Bedeutung zukommen. Wir wiederholen an dieser Stelle die Forderung, dass die Kantone Gelegenheit erhalten müssen, sich zu den Ausführungsvorschriften zu äussern. Auch auf die bereits angesprochene Kostenbeteiligung des Bundes sei hier nochmals ausdrücklich hingewiesen. Im Einzelnen ist Folgendes zu bemerken:

Zu Abs. 1 OR: Die Archivierung sowie der Austausch von elektronischen Daten werden auf einer vom Bundesrat vorgegebenen gesamtschweizerischen Norm

erfolgen müssen, damit der Datenaustausch zwischen den Handelsregisterbehörden in der Praxis funktioniert.

Zu Abs. 2 OR: Einer der Gründe für die Entstehung der Handelsregisterämter war es, im Dienste eines geordneten Geschäftsverkehrs, die Grundlage für den Nachweis zu schaffen, ob eine bestimmte Person berechtigt ist, einen im Register eingetragenen Rechtsträger zu vertreten und zu verpflichten. Zu diesem Zweck werden die eigenhändigen Unterschriften beglaubigt und beim Handelsregister hinterlegt. Da die Geschäfte immer mehr auf elektronischem Wege abgewickelt werden, vermag die blosse eigenhändige Unterschrift immer weniger zu genügen. Es stellt sich deshalb die Frage, ob für die im Handelsregister eingetragenen Personen nicht nur die eigenhändige Unterschrift zu hinterlegen, sondern gleichzeitig auch digitale Signaturen zu deponieren bzw. herauszugeben sind. Weiter sollte geprüft werden, inwieweit im Bereich des Handelsregisters ganz spezifisch auf die Aufgaben und Dienstleistungen im Bereich des Handelsregisterwesens zugeschnittene Zertifizierungsdienstleistungen angeboten werden könnten. Die Handelsregisterämter scheinen dazu durchaus in der Lage zu sein.

TI Contrariamente all'art. 942 cpv. 3 CC, questa norma introduce l'obbligo per i Cantoni di adeguarsi alla firma elettronica non appena lo deciderà la Confederazione. Gli uffici dei registri scambiano già dati in forma elettronica e non sembra che vi saranno problemi tecnici insormontabili per introdurre le nuove norme. Non è tuttavia possibile formulare già sin d'ora previsioni attendibili sui costi e sui tempi necessari per l'aggiornamento dei programmi informatici e delle strutture attuali alle nuove esigenze.

Rimane da definire in modo uniforme, a nostro parere, il momento preciso in cui la richiesta elettronica giunge all'ufficio. Come esposto in precedenza, riteniamo che tale momento debba coincidere con l'apertura del messaggio da parte del responsabile del registro di commercio (negli orari in cui il registro di commercio destinatario dell'invio è aperto al pubblico).

ZG In zeitlicher Hinsicht dringlich und mit den geringsten Umstellungen machbar erscheint insbesondere die Bestellung bzw. Auslieferung von Handelsregisterauszügen auf elektronischem Weg. Diesbezüglich sieht der Entwurf eine ausdrückliche gesetzliche Regelung vor (Art. 929a E-OR) bzw. eine Delegation an den Bundesrat, welcher die dazugehörigen Einzelheiten zu regeln hat. Sinnvollerweise wird der Bundesrat den Kantonen die Einführung beglaubigter, elektronisch signierter Handelsregisterauszüge ausdrücklich vorschreiben, um damit eine gesamtschweizerisch einheitliche Lösung zu fördern. Allerdings sollte den Kantonen dabei eine angemessene Übergangsfrist für die Einführung elektronischer Handelsregisterauszüge zugestanden werden.

<u>Organisationen / Organisations / Organizzazioni</u>

CP Cette norme invite le Conseil fédéral à édicter des prescriptions concernant la tenue électronique du registre du commerce. Nous n'y voyons pas d'inconvénient.

FGSec Die Begriffe „digitale Signatur“ / „elektronische Signatur“ werden inkonsistent verwendet.

SVV „[2] *Der Bundesrat bestimmt, ob und unter welchen Voraussetzungen*

a. die elektronische Einreichung von Anmeldungen und Belegen beim Handelsregister zulässig ist und

b. *elektronische Handelsregisterauszüge den beglaubigten gleichgestellt werden können.*

Er kann den Kantonen die Ausstellung elektronischer Handelsregisterauszüge vorschreiben."
Begründung: Nebst dem Entscheid des Bundesrates über die Voraussetzungen für eine zulässige elektronische Einreichung von Anmeldungen und Belegen beim Handelsregister sollte er sich auch über die Gleichstellung der elektronischen mit den beglaubigten Auszügen äussern. Dadurch erhält die Bestimmung klare Konturen und es würde sich auch die eher schwerfällige Beschreibung der beglaubigten, elektronisch signierten Handelsregisterauszüge in Absatz 2 erübrigen. Abgesehen davon dürfte die elektronische Zertifizierung eine Beglaubigung ohnehin ersetzen.

322.33 Art. 931 Abs. 2bis / Art. 931 al. 2bis / Art. 931 cpv. 2bis

Kantone / Cantons / Cantoni

BL Ebenfalls begrüsst wird die Möglichkeit des Bundesrates, die im Schweizerischen Handelsamtsblatt veröffentlichten Daten dem Publikum auch in elektronischer Form mit den entsprechenden Abfragemöglichkeiten zur Verfügung zu stellen (Art. 931 Abs. 2bis VE OR). Dies und insbesondere auch die Einrichtung eines „alert-Systems", mit welchem Publikationen betreffend bestimmter Geschäftspartner verfolgt werden können, entspricht einem von der Wirtschaft mehrfach geäusserten Bedürfnis. Es ist sinnvoll, dieses Bedürfnis gesamtschweizerisch abzudecken.

GR Art. 931 Abs. 2bis OR: Sollte der Bund die von den kantonalen Handelsregisterämtern aufbereiteten Daten in besonderer Form Interessenten aus der Privatwirtschaft zur Verfügung stellen und ergeben sich aus dieser Dienstleistung Einnahmen oder andere Vorteile, wie der Bezug von Informationen zu Vorzugskonditionen, die die privaten Dienstleister zusammenstellen (z.T. TELEDATA/KISS direct), ist es gerechtfertigt, dass die Kantone daran anteilmässig partizipieren können.

Organisationen / Organisations / Organizzazioni

CP Nous n'y voyons pas d'inconvénient.

322.4 Art. 16a Topographiengesetz
Art. 16a Loi sur les topographies
Art. 16a Legge sulle topografie

Kantone / Cantons / Cantoni

TI Non abbiamo osservazioni da formulare.

Organisationen / Organisations / Organizzazioni

CP Un nouvel article sur la communication électronique avec les autorités est inséré dans la loi sur les topographies, la loi sur la protection des marques et la loi sur les brevets. Nous n'y voyons pas d'inconvénient si ce n'est le fait que la communication électronique avec l'autorité ne doive pas donner lieu au paiement d'émolument. Il n'y a pas de raison de changer la procédure actuelle en la matière.

322.5 Art. 40 Markenschutzgesetz
Art. 40 Loi sur la protection des marques
Art. 40 Legge sulla protezione dei marchi

Kantone / Cantons / Cantoni

TI Non abbiamo osservazioni da formulare.

Organisationen / Organisations / Organizzazioni

CP Vgl. zu Art. 16a Topografiengesetz / Cf. ad art. 16a loi sur les topographies / Cfr. ad art. 16a legge sulle topografie.

322.6 Art. 65a Patentgesetz
Art. 65a Loi sur les brevets d'invention
Art. 65a Legge sui brevetti

Kantone / Cantons / Cantoni

TI Non abbiamo osservazioni da formulare.

Organisationen / Organisations / Organizzazioni

CP Vgl. zu Art. 16a Topografiengesetz / Cf. ad art. 16a loi sur les topographies / Cfr. ad art. 16a legge sulle topografie.

33 Weitere Vorschläge / Autres propositions / Altre proposte

Gerichte / Tribunaux / Tribunali

BGr In organisatorischer Hinsicht steht die Vorlage in einem engen Zusammenhang mit dem Entwurf für das neue Bundesgerichtsgesetz. Darin wird die Rechtsgrundlage für die rechtsgültige Einreichung von Rechtsschriften beim Bundesgericht und die rechtsgültige Zustellung von Urteilen auf elektronischem Weg geschaffen. Dieses Gesetz wird voraussichtlich erst erhebliche Zeit nach dem Bundesgesetz über die elektronische Signatur in Kraft treten. Dem Vernehmen nach bestehen daher Absichten, die entsprechenden Bestimmungen aus dem E des BGG vorzuziehen (Art. 36 Abs. 2, Art. 39 Abs. 4, Art. 56 Abs. 3 E BGG) und mit dem Bundesgesetz über die elektronische Signatur in Kraft zu setzen. Ein Herausbrechen einzelner Teile aus dem gesamten Reformpaket des BGG darf indessen nur nach eingehender Prüfung und im Einvernehmen mit dem Bundesgericht stattfinden. Die Einführung von elektronischen Eingaben ist für jedes Rechtsmittel mit einem erheblichem technischen Aufwand verbunden. Es muss daher vermieden werden, dass dieser Aufwand zunächst für die heutigen Rechtsmittel und kurze Zeit später für die neuen Rechtsmittel gemäss BGG geleistet werden muss.

Kantone / Cantons / Cantoni

AG Die gesetzliche Regelung steht dem technologischen Fortschritt insgesamt nicht im Weg. Zur generellen Verbreitung der digitalen Signatur ist jedoch vorab erforderlich, dass der Bund in Zusammenarbeit mit internationalen Gremien benutzerfreundliche Technologien fördert und technische Komponenten zertifizieren hilft. Bereits eingeleitete Aktivitäten in dieser Richtung, etwa im Projekt „guichet virtuel“, sind zu verstärken. Viel häufiger und wichtiger wird der Einsatz der digitalen Signatur aber zur Identifikation oder für sichere E-Mail und zum Abschluss formloser Verträge sein. Hier wird sie zu einem zentralen Instrument des Datenschutzes. Aus Sicht der Kantone ist es daher vordringlich, dass der digitalen Signatur durch die Förderung sicherer Komponenten zum Durchbruch verholfen wird.

BE Aus unserer Sicht ist davon auszugehen, dass mit den neu geschaffenen technischen Möglichkeiten auch neue Formen des Missbrauchs auftreten werden. Die Strafrechtspflege wird sich vor allem im Bereich der Wirtschaftskriminalität und der Urkundendelikte mit der neuen Erscheinung der elektronisch signierten Computerurkunden vermehrt auseinandersetzen müssen, soweit sie es nicht bereits heute tut. Die bestehenden strafrechtlichen Grundlagen und die Lehre dazu, beides in Verbindung mit dem darauf abgestimmten BGES resp. der Teilrevision von OR und UWG sind unseres Erachtens ausreichend.

BL Die gesetzliche Regelung steht dem technologischen Fortschritt insgesamt nicht im Weg. Zur generellen Verbreitung der elektronischen Signatur ist aber nötig, dass der Bund (wohl in Zusammenarbeit mit internationalen Gremien) benutzerfreundliche Technologien fördert und technische Komponenten zertifizieren hilft. In diese Richtung bereits eingeleitete Aktivitäten – etwa im Projekt „guichet virtuel“ – sind noch zu verstärken. Wird mit der elektronischen Signatur die handschriftliche Unterschrift bei Vertragsschlüssen ersetzt, bildet dies gleichsam den „oberen Abschluss“ des Einsatzumfelds der elektronischen Signatur. Viel häufiger und wichtiger wird der Einsatz der elektronischen Signatur aber zur Identifikation oder für sicheres E-Mail und zum Abschluss formloser Verträge sein. Hier wird sie zu einem zentralen Instrument des Datenschutzes. Aus Sicht der Kantone ist es daher vordringlicher, dass der elektronischen Signatur durch die Förderung sicherer Komponenten zum Durchbruch verholfen wird. Der Gesetzesentwurf bietet Gelegenheit dazu, dies in Erinnerung zu rufen.

BS Dank der elektronischen Signatur erhält nun der Empfänger einer elektronisch übermittelten Willenserklärung die Gewissheit, dass die Willenserklärung von einer bestimmten Person abgesandt worden ist und unverändert bei ihm eingetroffen ist. Der Preis, den der Empfänger für diese Gewissheit bezahlen muss, ist im Gesetz nicht festgelegt; er richtet sich nach Angebot und Nachfrage. Wie der Staat für öffentliche Beurkundungen - ob sie durch private Notare oder durch staatliche Amtsnotare erfolgen - die Tarife festsetzt, so sollte der Staat im Gesetz auch die Tarife für die Zertifizierungsdienste festsetzen.

Um die rechtlichen und technischen Fragen im Zusammenhang mit der Einreichung von elektronisch signierten Anmeldungen und Belegen regeln zu können, wird eine Arbeitsgruppe oder eine Kommission zu bilden sein. Diese Arbeitsgruppe sollte sowohl aus Juristinnen und Juristen und Handelsregisterfachleuten als auch aus Personen zusammengesetzt sein, welche über die in diesem Bereich erforderlichen technischen Fachkenntnisse verfügen. Auf diese Weise könnte sowohl die bundesrätliche Verordnung wie auch die Weisung an die Handelsregisterbehörden so vorbereitet werden, dass die bestmögliche Realisierung sichergestellt wäre. Von der Berufung von zwei Kommissionen (Handelsregisterfragen und technische Fragen) ist deshalb abzuraten, weil die Verbindung zwischen juristischen und technischen Fragen im vorliegenden Zusammenhang sehr eng ist.

TI Il progetto propone un sistema complesso di responsabilità, che tiene conto solo delle possibilità di abuso o di danno derivante dall'uso improprio della firma elettronica soggetto alla normativa specifica. Ci permettiamo di suggerire, visti i delicati problemi che possono sorgere in questo settore (per esempio in caso di concorso di responsabilità fra l’utente e il prestatore di servizi di certificazione) e le difficoltà tecniche poste dall'onere di provare fatti tecnici complessi, l'inserimento nella legge di norme che precisino le responsabilità rispettive quando il danno è causato da altri fattori (interpolazione, mutilazione o altre modifiche del

testo preceduto dalla firma elettronica), con un rinvio alle norme generali del Codice delle obbligazioni.

A nostro avviso à anche auspicabile precisare nella legge il foro e il diritto applicabile quando il prestatore di servizi di certificazione risiede all'estero, opera all'estero o impiega personale fuori dal territorio svizzero.

VS Enfin, le rapport ne comporte pas la traditionnelle partie relative aux incidences au niveau des cantons. On ne saurait toutefois méconnaître l'effet réflexe de la possibilité ouverte au plan privé sur les actes cantonaux de droit public et de droit privé, de sorte que les propositions relatives à la signature des actes de procédure ou autres documents devraient très rapidement suivre, avec des systèmes simples, largement répandus mais ouverts. Dans ce sens, le Conseil d'Etat prend acte des déclarations du Département fédéral de justice et police selon lesquelles „les autres questions, comme par exemple l'acceptation du dépôt d'un mémoire ou de la notification d'une décision par la voie électronique, seront réglées dans d'autres lois“. Puisse le législateur fédéral faire diligence, en particulier à l'occasion des lois fédérales sur la procédure civile et pénale (art. 122 al. 1 et 123 nCst. révisés).

Organisationen / Organisations / Organizzazioni

EKK Les normes du projet de loi relatives à la surveillance des fournisseurs de services de certification reconnus et à la responsabilité sont très importantes. En effet, comme mentionné dans le commentaire, elles constituent les conditions optimales aptes à garantir la sécurité des actes juridiques effectués par la voie électronique.

La Commission demande qu'au moment où cette loi entrera en vigueur, les consommateurs soient informés précisément de la responsabilité du titulaire de la clé privée. A cet effet, il faudra que les titulaires d'une clé privée apprennent de façon concrète à conserver leur clé privée de manière à en prévenir toute utilisation abusive par un tiers.

FGSec Die Problematik eines unakkreditierten CSP, welcher qualifizierte Zertifikate ausstellt, muss ebenfalls noch behandelt werden.

Der Inhalt des Begleitberichts deckt zum Teil Fragestellungen unterschiedlicher Tiefe in einer nicht nachvollziehbaren Form ab, und ist in der aktuellen Version nicht akzeptabel. Z.B. erklärt 142.2 exzellent und nachvollziehbar die Auswirkungen auf die Willenserklärung und Haftung. Die in 210.071 genannten Beispiele, „Sein Leben zu riskieren" und in 210.073 „Stromunterbruch", sind in der vorliegenden Art aber zu grob, decken die eigentlichen Problematiken nicht ab und diskreditieren den Rest des Dokuments.

Eine angemessene Behandlung des Problems der Unterwanderung eines Systems (Trojanische Pferde etc.) fehlt hingegen.

KPMG Da grundsätzlicher Natur, möchten wir an dieser Stelle zwei Anliegen anbringen: Erstens sollten die allgemeinen Bestimmungen des Vertragsrechts nur soweit geändert bzw. ergänzt werden, als dies für die rechtliche Gleichstellung der elektronischen mit der eigenhändigen Signatur unbedingt notwendig ist. Damit soll nicht nur der Bruch mit bewährten, historisch gewachsenen Rechtsinstitutionen verhindert werden, sondern auch gewährleistet sein, dass Lehre und Rechtsprechung im grösstmöglichen Umfang übernommen und weitergeführt werden können. Zweitens soll durch die für schweizerische Verhältnisse relativ schnelle Gangart einer Gesetzesanpassung nicht ausser Acht gelassen werden, dass eine grundsätzlichere Überarbeitung der Formvorschriften folgen muss. Die

Erleichterung der Kundgabe formbedürftiger Willenserklärungen kann auf zwei Wegen erfolgen: Erstens können die Formerfordernisse beseitigt oder herabgestuft (aus qualifizierter Schriftlichkeit wird einfache Schriftlichkeit, aus Schriftlichkeit wird Textform, d.h. eine in lesbaren Schriftzeichen fixierte Erklärung (der deutsche „Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr“ [Stand: 6. September 2000] [„D-Entwurf“] definiert in § 126b die Textform als eine in Schriftzeichen lesbare, die Person des Erklärenden angebende und den Abschluss der Erklärung in geeigneter Weise erkennbar gemachte Erklärung“) und zweitens können die möglichen Schriftformen durch eine weitere Möglichkeit, bspw. die digitale Signatur, erweitert werden. Der vorliegende Gesetzesentwurf beschränkt sich - aus zeitlichen Gründen - zu Recht auf die zweite Option. Nichtsdestoweniger sollten mittelfristig die zahlreichen Gesetzesbestimmungen mit Formvorschriften auf ihre Notwendigkeit hin überprüft werden.

SAV L’activité de certification de signatures s’apparente à la légalisation d’une signature par un notaire. Il s’agit d’une activité quasi-officielle, même si elle est exercée par des sociétés privées. En raison des contraintes imposées par la LFSél, il est peu probable que les fournisseurs de services de certification soient nombreux. Il y a donc un risque sérieux que les différentes régions linguistiques n’aient pas un accès égal aux services de certification de signature. En l’absence de dispositions dans la LFSél comparables à celles que l’on trouve dans la législation sur les assurances (cf. RS 961.01 – chapitre 5), les Suisses de langue française ou italienne ne pourront probablement avoir accès aux services de certification qu’en acceptant d’être liés par des contrats dont seule la version allemande fera foi et qui seront de surcroît soumis au for exclusif de Zurich. Sans intervention du législateur, il y a un risque réel de créer une Suisse à deux vitesses. Les conditions générales de Swisskey sont un exemple éloquent de cette évolution.

Enfin, pour limiter la tentation de transfert des activités de certification à l’étranger, et surtout pour protéger les utilisateurs suisses, il conviendrait de prévoir un for impératif au domicile de l’utilisateur suisse pour les procédures judiciaires relatives aux services de certification. Pour le surplus, le fournisseur étranger qui refuserait le for en Suisse pourrait accompagner son certificat d’une déclaration excluant de ses services les résidents suisses (comme les banques suisses doivent exclure les résidents US des offres de souscription non conforme à la législation US).

Schlauri/Kohlas Die grosse Bedeutung der Schriftform im Privatrechtsverkehr basiert nicht nur auf deren Einsatz bei formbedürftigen Rechtsgeschäften, sondern auch auf deren freiwilligem Einsatz im formfreien Bereich und auf der besonderen Stellung der Urkunde im Prozess- und Betreibungsrecht. Damit stellt sich insbesondere auch die Frage nach der prozessrechtlichen Anerkennung digital signierter Dokumente als Urkunden.

Der Begleitbericht zum VE-BGES geht davon aus, dass mit einer zivilrechtlichen Gleichsetzung der digitalen Signatur durch einen neuen Art. 15a OR auch eine solche im prozessualen Bereich bewirkt werde, d.h. dass ein digital signiertes Dokument als Urkunde im Beweisverfahren und etwa als schriftliche Schuldanerkennung im SchKG anerkannt sei, zumindest soweit die entsprechenden kantonalen oder eidgenössischen Normen direkt oder indirekt auch auf die Formvorschriften des Obligationenrechts Bezug nehmen (Begleitbericht, 142.2.). Dabei wird jedoch übersehen, dass für eine prozessrechtliche Aner-

kennung eines Dokumentes als Urkunde nicht nur Schriftlichkeit, sondern auch eine Verkörperung notwendig ist, d.h. die Verbindung der Erklärung mit einem physischen Träger, der Verkehrsfähigkeit und Lesbarkeit der Urkunde aus sich heraus sicherstellt. Erst sie rechtfertigt die Privilegierung der Urkunde gegenüber anderen Beweismitteln (etwa bezüglich Zulässigkeit im summarischen Verfahren oder Beweiskraft).

Die digitale Signatur ist zumindest bezüglich der einfachen Handhabung der Handunterschrift nicht ebenbürtig, weil es ihr an der erwähnten Verkörperung mangelt und zu ihrer Überprüfung immer eine Computerausrüstung nötig ist. Anders als D. Gasser annimmt, kann eine digitale Signatur u.E. nicht einfach ausgedruckt und hernach dem Richter zur visuellen Prüfung vorgelegt werden, denn es wäre ein Leichtes, ein einem solchen Ausdruck, der nur die Nachricht enthält und irgendwo ein grafisches Symbol als Zeichen für die Signatur, täuschend ähnliches Papierdokument auf einer ganz normalen Textverarbeitung zu erstellen. Der Ausdruck einer digitalen Signatur ist damit nicht sicherer als ein ausgedrucktes unsigniertes digitales Dokument und zum Urkundenbeweis nicht zuzulassen.

Den Gerichten werden zu einer elektronischen Überprüfung vorläufig regelmässig Know-how und Infrastruktur fehlen, so dass Sachverständigengutachten einzuholen sind. Ob die daraus entstehenden Schwierigkeiten im Rahmen eines Verfahrens in Kauf genommen werden müssen, das eigentlich auf einen herkömmlichen Urkundenbeweis ausgelegt ist, ist u.E. durch die zivilrechtliche Anerkennung der digitalen Signatur im OR nicht entschieden (gl.M. etwa J. Bizer/V. Hammer, Elektronisch signierte Dokumente als Beweismittel, Datenschutz und Datensicherung 11/1993, 619 ff.).

Ein möglicher Lösungsansatz ergibt sich aber bereits aus Art. 21 VE-BGES: Gemäss dieser Bestimmung bestätigt die Akkreditierungsstelle (oder eine andere, vom Bundesrat bezeichnete Stelle) gegen Gebühr, dass die auf einem digitalen Dokument vorhandene digitale Signatur auf dem Wege eines gesetzeskonformen Verfahrens und mit einem gültigen Zertifikat erstellt wurde. Diese Bestätigung wird als Papierurkunde ausgefertigt, welche in einem Prozess dann natürlich als solche eingesetzt werden kann (es handelt sich dabei ja – anders als bei Gasser – nicht bloss um einen durch eine Partei erstellten Ausdruck der signierten Nachricht, sondern um eine Bestätigung von dritter Stelle, dass die elektronische Überprüfung einer Signatur erfolgreich war). Um die geschilderten Schwierigkeiten zu vermeiden, sollte der urkundenmässige Einsatz digital signierter Dokumente im Prozess vorläufig nur mittelbar auf dem Wege einer solchen Bestätigung zugelassen werden. Eine unmittelbare prozessrechtliche Anerkennung der digitalen Signatur sollte erst dann erfolgen, wenn die Gerichte mit den zu einer unmittelbaren Prüfung notwendigen Mitteln ausgestattet sind.

Zu beachten ist ferner, dass es sich bei der Konformitätsbestätigung i.S.v. Art. 21 VE-BGES nicht um die Originalurkunde, sondern bloss um ein Surrogat handelt, das als solches de lege lata womöglich zum Beweis gar nicht zugelassen wäre. Diese Bestätigung ist nur ein schriftliches Sachverständigengutachten über das Vorliegen einer Urkunde. Die Zulassung zum Urkundenbeweis ist daher u.E. explizit durch Gesetz vorzusehen, um jegliche Rechtsunsicherheit auszuschliessen.

Damit ergibt sich der folgende Vorschlag zu einem Art. 21 Abs. 4 VE-BGES, der eine mittelbare prozessrechtliche Anerkennung bewirkt:

[4]Die Bestätigung gemäss Absatz 1 ist als Surrogat des digitalen Dokumentes zum Urkundenbeweis zugelassen.

Die unmittelbare Anerkennung digital signierter Dokumente hingegen sollte den kantonalen Gesetzgebern überlassen bleiben, bzw. erst im Rahmen der gesamteidgenössischen ZPR-Kodifikation erfolgen.

SUISA Wir würden es deshalb sehr begrüssen, wenn der Anwendungsbereich der elektronischen Signatur einzelgesetzlich bestimmt, insbesondere Art. 82 SchKG entsprechend angepasst würde.

SVV Revision des Versicherungsvertragsgesetzes

Vorbemerkung: In Anbetracht des geltenden Versicherungsvertragsgesetzes (VVG) und der durch die laufende Teilrevision dieses Gesetzes vorgesehenen Änderungen drängen sich für elektronische Lösungen im Versicherungsbereich einige Anpassungen im VVG auf. Der SVV hat sich zu den fraglichen Punkten bereits in der Vernehmlassung zur Teilrevision des VVG geäussert. Dieses Projekt ist allerdings eine Folge der Totalrevision des Versicherungsaufsichtsgesetzes; lediglich die daraus fliessenden notwendigen Bestimmungen sollen angepasst werden. Damit dem elektronischen Geschäftsverkehr in der Versicherungsbranche nichts im Wege steht und die kritischen Regelungen auch nicht der Interpretation der Rechtsprechung überlassen werden müssen, beantragen wir an dieser Stelle folgende Änderungen:

Art. 3 VE-VVG Informationspflicht des Versicherers

Antrag: „[1]*Der Versicherer hat dem Versicherungsnehmer Informationen* über die Identität des Versicherers, über die versicherten Risiken, über die Leistungspflicht, über die Prämienzahlungen, über Laufzeit und Beendigung des Versicherungsvertrages sowie anwendbare Allgemeine Versicherungsbedingungen *zur Verfügung zu stellen*."

Begründung: Art. 3 Abs. 2 VE-VVG verlangt, dass die vorvertraglichen Informationspflichten dem Versicherungsnehmer so zu übergeben sind, dass er sie kennen kann, wenn er den Versicherungsvertrag beantragt oder annimmt und dass er zu diesem Zeitpunkt im Besitz der allgemeinen Versicherungsbedingungen ist. Um die Diskussion an dieser Stelle nicht erneut aufzurollen, verweisen wir grundsätzlich auf unseren Antrag in der damaligen Stellungnahme ans BPV. Darin haben wir zum Ausdruck gebracht, dass mit der gewählten Formulierung einerseits der bereits heute existierende Telefonverkauf und andererseits der „Electronic Commerce" verunmöglicht würde. Die Vorlage sei deshalb so auszugestalten, dass diese neuen Arten des Vertriebs realisiert werden können und der Konsumentenschutz dennoch gewährleistet bleibt.

Seitens des BPV wurde zugesichert, dass die Verwaltung alles daran setzen werde, um der Versicherungsbranche den Zugang zu einem kompletten elektronischen Geschäftsverkehr zu ermöglichen. Da gemäss neuesten Informationen dennoch keine Änderungen am Entwurf vorgesehen sind, wird die Frage der elektronischen Zustellung der vorvertraglichen Informationspflichten gezwungenermassen der Praxis überlassen bleiben. Im Sinne unserer Vernehmlassung zur Teilrevision des VVG, beantragen wir deshalb auch an dieser Stelle Art. 3 VE-VVG dem elektronischen Geschäftsverkehr anzupassen, indem der Versicherer dem Versicherungsnehmer die entsprechenden Informationen zur Verfügung zu stellen hat statt diese in Schriftform zu „übergeben" (relevant für den elektronischen Geschäftsverkehr ist dabei der rot markierte Teil der Bestimmung).

Art. 11 VVG

Antrag: „Der Versicherer ist gehalten, dem Versicherungsnehmer eine Police auszuhändigen *oder gemäss Art. 15a OR elektronisch signiert zuzustellen,* welche die Rechte und Pflichten der Parteien feststellt. Der Versicherer ist be-

rechtigt, vom Versicherungsnehmer ausser Porto und Stempelkosten eine Gebühr für Ausfertigung der Police sowie für Abänderungen derselben zu erheben. Die Höhe dieser Gebühr kann durch Verordnung des Bundesrates begrenzt werden.

Der Versicherer muss überdies dem Versicherungsnehmer auf Verlangen eine Abschrift der in den Antragspapieren enthaltenen oder anderweitig abgegebenen Erklärungen des Antragstellers, auf Grund deren die Versicherung abgeschlossen wurde, gegen Ersatz der Auslagen *zustellen*."

Begründung: In Art. 11 VVG sieht die laufende Teilrevision zum VVG keine Änderungen vor. Darin festgehalten ist die Zustellung der Police. Gemäss Begleitbericht zum BGES soll die Frage der elektronischen Zustellung der Police der Praxis überlassen werden. Eine wörtliche Interpretation der Bestimmung verlangt allerdings eine physische Aushändigung und ist so dem E-Commerce grundsätzlich hinderlich. Wir beantragen deshalb, die elektronisch signierte Zustellung der physischen Aushändigung mit einem entsprechenden Eintrag in Abs. 1 gleichzustellen. Konsequenterweise ist in Abs. 2 das Wort „aushändigen" durch „zustellen" zu ersetzen.

SwissICT Im Zusammenhang mit dem Zugang zu den Registern muss klargestellt werden, dass Einzelabfragen in der Regel kostenlos erfolgen, hingegen Massenabfragen und weitergehende Dienstleistungen verrechnet werden können.

TSM Der strafrechtliche Schutz von elektronischen Dokumenten ist wichtig. Die gesetzgeberische Lösung sollte die Gelegenheit nutzen und das elektronisch signierte Dokument auch ausdrücklich als Urkunde im Sinne des Strafgesetzbuches definieren. Sowohl der Tatbestand der Urkundenfälschung wie auch derjenige des Betruges sollten als wirksamer Schutz einer elektronischen Urkunde im Verletzungsfalle ausdrücklich herangezogen werden können.

Vischer Die Bestimmungen des Obligationenrechts über die Stellvertretung (Art. 32 ff. OR) sind mit einer Bestimmung zu ergänzen, wonach das befugte Handeln unter fremdem Namen, insbesondere das befugte Verwenden fremder Legitimationsmittel unter Abwesenden, die gleichen Rechtswirkungen hat wie das Handeln in fremdem Namen im Sinne von Art. 32 Abs. 1 OR.

Ein fremder Signaturschlüssel kann auch in befugter Weise, mit Ermächtigung des Schlüsselinhabers, verwendet werden. Es ist offensichtlich, dass das Instrument der elektronischen Signatur hervorragend dazu geeignet ist, auf schnelle und einfache Weise Rechtsgeschäfte durch einen Dritten, (z. B. durch einen Anwalt oder einen Treuhänder) abschliessen zu lassen. Dies wird in der Praxis immer mehr vorkommen, sobald sich der Austausch digital signierter Erklärungen im Geschäfts- und Rechtsverkehr faktisch durchgesetzt hat und sobald Behörden und Registerämter digital signierte Eingaben akzeptieren werden. Ungeachtet aller Sicherheitsbedenken ist zu erwarten, dass die elektronische Signatur als Mittel zur Stellvertretung eingesetzt werden wird.

Der vorliegende Gesetzesentwurf äussert sich nicht zu den Rechtswirkungen, die dadurch entstehen, dass der Inhaber eines Signaturschlüssels diesen einem Dritten zur Verfügung stellt, damit der Dritte mit Wirkung für den Prinzipal handeln kann. Zwar handelt es sich dabei um einen Vorgang, der sich im Prinzip auch ohne elektronische Signatur ereignen könnte; insofern hängt die sich dabei stellende Rechtsfrage nicht direkt mit dem hier diskutierten Gesetzesentwurf zusammen. Aber das Instrument der elektronischen Signatur eignet sich besonders gut zur befugten Fremdverwendung, weshalb der vorliegende Gesetzesentwurf einen geeigneten Anlass bietet, auf diese Konstellation einzugehen. Die Konstellation der befugten Verwendung eines auf eine fremde Person

hinweisenden Legitimationsmittels entspricht nicht der einer gewöhnlichen Stellvertretung. Bei der Stellvertretung wird davon ausgegangen, dass der Stellvertreter im Namen des Vertretenen handelt, dass also das Vertretungsverhältnis für Aussenstehende erkennbar ist (vgl. Art 32 OR). Gerade dies wird aber bei der Verwendung eines fremden Legitimationsmittels, namentlich einer fremden elektronischen Signatur, oft nicht der Fall sein, weil der Unterzeichnende nicht in fremdem Namen, sondern unter fremdem Namen auftritt. Das Stellvertretungsverhältnis wird dabei für Aussenstehende nicht erkennbar, sie erhalten den Eindruck, der Prinzipal selbst habe die Mitteilung signiert und verschickt.

Ob das befugte Handeln unter fremdem Namen als Spezialfall der Stellvertretung angesehen werden kann und demnach die in Art. 32 Abs. 1 OR vorgesehene Rechtsfolge nach sich zieht, wird in der Literatur kaum und jedenfalls nicht durchgehend positiv beantwortet (vgl. etwa GUHL/KOLLER, Das Schweizerische Obligationenrecht, 9. Aufl., Zürich 2000, § 19 N. 16; ZÄCH, Berner Kommentar, Bern 1990, N. 74 zu Art. 32 OR). Es würde sich daher rechtfertigen, die einschlägigen Bestimmungen des Obligationenrechts mit einer Bestimmung zu ergänzen, wonach das befugte Handeln unter fremdem Namen, insbesondere das befugte Verwenden fremder Legitimationsmittel unter Abwesenden, die gleichen Rechtswirkungen hat wie das Handeln in fremdem Namen im Sinne von Art. 32 Abs. 1 OR.