Glue Software Engineering

CMS-Attribute der Zulassungsbestätigung v3

Spezifikation

Version 1.0 / 30.08.2021

GLUE Software Engineering AG explicitly draws attention to possible changes of this document due to technical or functional progress without further notice and without Justification.

GLUE Software Engineering AG
Schwarztorstrasse 31
CH – 3007 Bern

Document Administration	
Author(s)	Adrian Greiler, Dr. Igor Metz
Doc.-Tool	Microsoft Word
Storage	G:\kunden\Bundesamt_fuer_Justiz\Notarenregister\11_UPReg_ohne_SuisseID\Spezifikation-CMS_Attribute\Spezifikation-CMS_Attribute_der_Zulassungsbestätigung_v3-2021-08-30.docx
Distribution	Bundesamt für Justiz, Glue Software Engineering AG

Version	1.0		**Release Date**		30.08.2021	
Function						
Date						
Signature						

Version History			
Version	**Description**	**Date**	**Initials**
0.1	Initiale Version	22.02.2016	AG
0.2	Review durch IM	23.02.2016	IM
0.3	Anpassungen gemäss Review durch IM	23.02.2016	AG
0.4	Beispiele hinzugefügt	26.02.2016	AG
0.5	Vorbereitung auf Release	07.10.2016	AG
0.6	Der Kanton wird seit ZulaB in die Signatur kodiert	17.10.2016	AG
0.7	Totalrevision für Zulassungsbestätigung Version 3	24.11.2020	AG,IM
0.8	Korrektur der Kapselung der Claimed Attributes innerhalb der ASN1-Struktur. Entfernen missverständlicher Beispiele seit Hinzufügung von LTV-Informationen	18.08.2021	AG
1.0	Korrekturen	30.08.2021	IM

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1. Einführung

Das Urkundspersonenregister (UPReg) bestätigt die Zulassung einer Urkundsperson mit einer zusätzlichen Signatur auf einem qualifiziert signierten Dokument. Die zusätzliche Signatur wird mit der Cygillum Clientanwendung oder durch eine Software von Drittanbietern im Zusammenspiel mit einem Webservice des UPReg angebracht. Dabei prüft UPReg die Signatur der Urkundsperson (erste Signatur) und signiert seinerseits das Dokument (zweite Signatur) erneut, um die Zulassung der Urkundsperson zu bestätigen.

Das Problem hierbei ist, dass UPReg die zweite Signatur erstellt, ohne das Originaldokument in Händen zu halten. Der Ablauf unter Verwendungen der Cygillum Clientanwendung ist wie folgt:

1) Urkundsperson signiert ein PDF-Dokument (qualifizierte Signatur).
2) Urkundsperson fordert softwaregestützt die Zulassungsbestätigung an.
3) Die Software startet auf UPReg eine Session und schickt die Urkundsperson auf die Webseite von UPReg, damit sie sich dort authentisiert.
4) Die Software errechnet sodann den zu signierenden Hash des (qualifiziert signierten) PDF.
5) Die Software fordert für den Hash eine Zulassungsbestätigung für die Urkundsperson an, welche qualifiziert signiert hat und sich gegenüber dem System auf dessen Webseite mit zwei Faktoren authentisiert hat.
6) UPReg prüft die Berechtigung anhand des Zertifikats in der qualifizierten Signatur, signiert den Hash und gibt die Signatur der Zulassungsbestätigung zurück.
7) Die Software bettet die Signatur von UPReg in das Dokument ein.

Mit einer speziell dafür erstellten Software wäre es möglich, den Hash eines anderen Dokuments an UPReg zu senden und die Zulassungsbestätigungssignatur in dieses Dokument einzufügen. Dadurch entsteht ein Dokument, das von einer Software zur Validierung von Signaturen fälschlicherweise als ein gültiges elektronisches notarielles Dokument erkannt würde.

Damit der Signaturvalidator erkennen kann, auf welche Urkundsperson sich die Signatur der Zulassungsbestätigung bezieht, sind zusätzliche Informationen als Sicherheitselemente in die Signatur der Zulassungsbestätigung eingebettet. Damit Veränderungen an diesen Informationen erkannt werden können, werden sie signiert und als sogenannte CMS Signed Attributes in der Zulassungsbestätigung eingebettet.

Die Implementierung der Zulassungsbestätigung v3 des UPReg geht mit dem UPReg Change 2020/2021 und der Anforderung einher, dass die Signatur des UPReg LTV-fähig sein muss. Das vorliegende Dokument beschreibt die sogenannten CMS Signed Attributes, die in der Zulassungsbestätigung als Sicherheitselement verwendet werden. Die CMS Signed Attributes der Zulassungsbestätigung v3 unterscheiden sich von denen der Zulassungsbestätigung v2. Vor der dritten Version wurden die CMS Signed Attributes nicht als Claimed Attributes, sondern direkt als Signed Attributes hinterlegt.

2. Einordnung

Digitale Signaturen speichern die benötigten Informationen und Werte in einer sogenannten ASN1-Struktur. Darin können, neben den Standartattributen wie dem Hash der Signatur, der Signatur selbst, der Timestamp-Informationen usw., auch proprietäre Informationen abgelegt werden. Dafür bietet ASN1 eine Baumstruktur an, in welcher die Werte über einen Schlüssel abgelegt sind und wieder angesprochen werden können. Diese Schlüssel heissen Object Identifier (OID). Die Elemente dieser OID bezeichnen eine Baumstruktur, die Knoten sind durch Punkte getrennt.

2.1. Claimed Attributes

Das RFC-3126[1] definiert hierfür die Claimed Attributes innerhalb des Knotens Signer Attributes mit der OID 1.2.840.113549.1.9.16.2.18.

[1] https://datatracker.ietf.org/doc/html/rfc3126#section-3.12.3

Die nachfolgend aufgeführten Attribute werden darin als Attribute mit einem einzigen Wert eingetragen.

2.2. OID-Pfad für UPReg

Für UPReg wird folgender OID-Pfad verwendet:

`2.25.155567022322770787173630853582050149659`

Dieser wurde gemäss http://www.oid-info.com/faq.htm#10 aus einer zeitstempelbasierten UUID generiert. Die einzelnen Attribute sind darunter angesiedelt.

2.3. Struktur

Unter dem OID-Pfad für UPReg sind die einzelnen Werte (vom Typ DEROctetString) mit folgenden OIDs abgelegt:

OID	Beschreibung
`2.25.155567022322770787173630853582050149659.1`	Transaktions-ID (UUID v4) welche die Aufrufe der Webservices zur Anbringung der Zulassungsbestätigung identifiziert. Diese findet sich in den Logs und Protokollen wieder.
`2.25.155567022322770787173630853582050149659.2`	Timestamp der Anfrage (Unix-Time in Millisekunden)
`2.25.155567022322770787173630853582050149659.3`	Domäne, für welche diese Zulassungsbestätigung ausgestellt wurde. Entspricht dem JSON Attribut *domain* beim Aufruf des Webservices für die Zulassungsbestätigung.
`2.25.155567022322770787173630853582050149659.4`	X509-Issuer des Zertifikats der Signatur der Urkundsperson, auf welche sich diese Zulassungsbestätigung bezieht. Dieses Attribut wird aus dem JSON Attribut *pkcs7* beim Aufruf der Methode „rt1-generate“ des Webservices für die Zulassungsbestätigung extrahiert. Im Attribut *pkcs7* ist die Signatur der Urkundsperson enthalten.
`2.25.155567022322770787173630853582050149659.5`	X509-Subject des Zertifikats der Signatur der Urkundsperson, auf welche sich diese Zulassungsbestätigung bezieht. Dieses Attribut wird aus dem JSON Attribut *pkcs7* beim Aufruf der Methode „rt1-generate“ des Webservices für die Zulassungsbestätigung extrahiert. Im Attribut *pkcs7* ist die Signatur der Urkundsperson enthalten.
`2.25.155567022322770787173630853582050149659.6`	X509-Serial des Zertifikats der Signatur der Urkundsperson, auf welche sich diese Zulassungsbestätigung bezieht. Dieses Attribut wird aus dem JSON Attribut *pkcs7* beim Aufruf der Methode „rt1-generate“ des Webservices für die Zulassungsbestätigung extrahiert. Im Attribut *pkcs7* ist die Signatur der Urkundsperson enthalten.

OID	Beschreibung
2.25.155567022322770787173630853582050149659.7	Kanton, für welche diese Zulassungsbestätigung ausgestellt wurde. Entspricht dem JSON Attribut *canton* beim Aufruf des Webservices für die Zulassungsbestätigung.

Tabelle 1: Object Identifier der Signed Attributes der Zulassungsbestätigung

2.4. Struktur der Signed Attributes unter der UPReg-OID

Folgendes Beispiel zeigt den Ast der Struktur, welche von UPReg gesetzt wird. Diese Werte werden für die Validierung gegenüber der Signatur der Urkundsperson verwendet.

```
└2
 └25
   └155567022322770787173630853582050149659
                                              ├1   Transaktions-ID
                                              ├2   Timestamp
                                              ├3   UPReg-Domain
                                              ├4   X509-Issuer
                                              ├5   X509-Subject
                                              ├6   X509-Serial
                                              └7   Kantonskürzel
```

Abbildung 1: OID-Struktur von UPReg in Signatur Zulassungsbestätigung

2.5. Beispiel möglicher Werte in Claimed Attributes

Beispiele für die Werte, welche für die Validierung der Signatur verwendet werden:

- Transaktions-ID: 20d8c611-b841-4266-8378-34783eb2b875
- Timestamp: 1456154449123
- UPReg-Domain: upreg
- X509-Issuer: CN=SwissSign Platinum CA - G2,O=SwissSign AG,C=CH
- X509-Subject: SERIALNUMBER=1200-2533-4423-9485, E=ag@glue.ch, CN=Adrian Matthias Greiler (Qualified Signature)
- X509-Serial: 888913183433941903900774700668947901
- Kantonskürzel: BE

Die ersten drei und der letzte Wert sind dabei lediglich Zusatzinformationen, welche dazu dienen, bei einem Supportfall oder einer Fälschung schneller den dazugehörigen Logeintrag zu finden. Die drei unteren (Präfix *X509*) beziehen sich dagegen direkt auf die Signatur der Urkundsperson und müssen mit den Informationen des Zertifikats dieser Signatur übereinstimmen. Stimmen diese Werte nicht überein, kann von einer Fälschung ausgegangen werden.

2.6. Beispiel der Signaturen und Claimed Attributes auf dem Dokument

Die folgende Abbildung zeigt ein Beispiel zur Veranschaulichung der referenzierten Attribute und deren Werte:

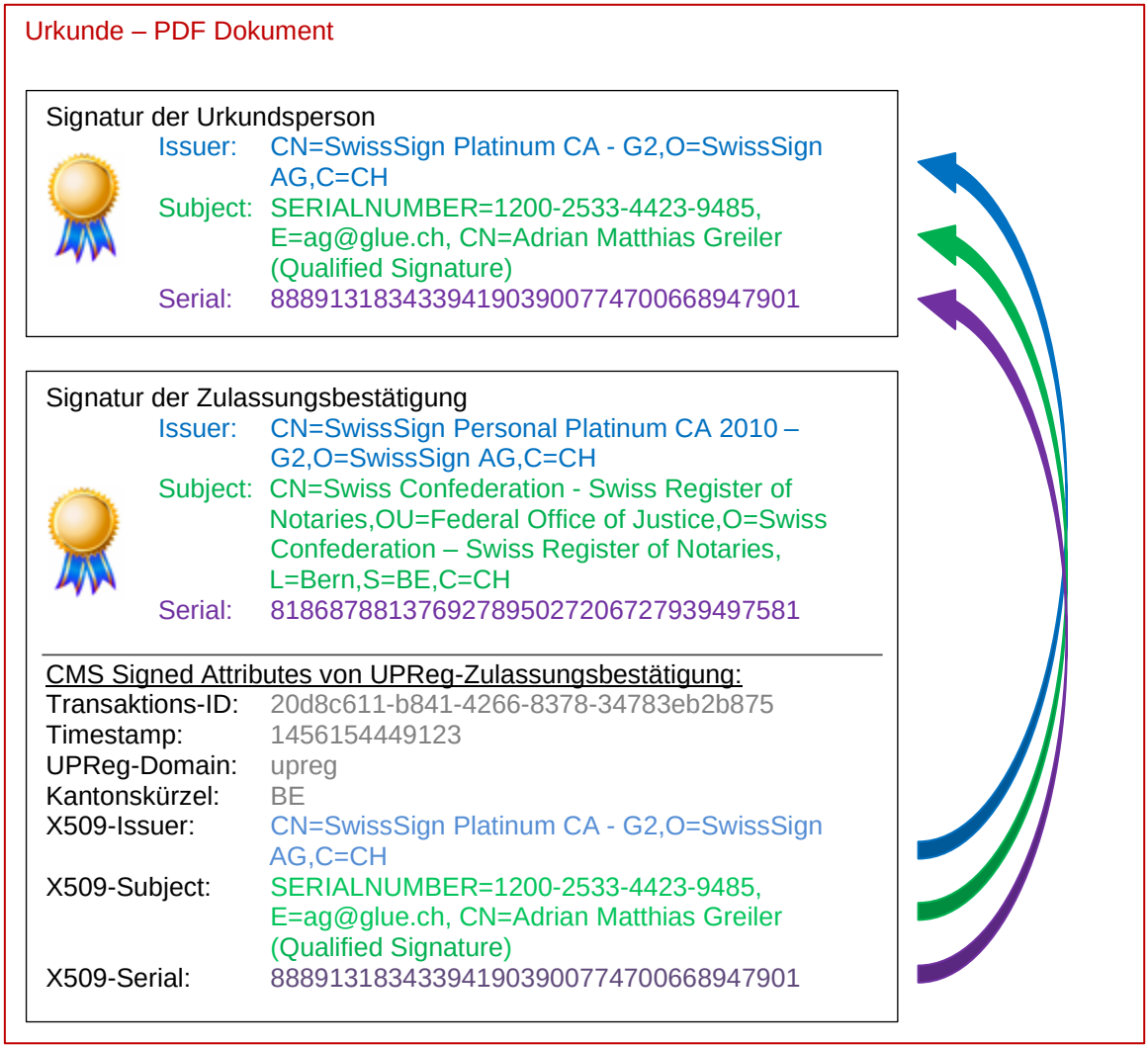

Abbildung 2: Beispiel der Referenzen der CMS Signed Attributes

In diesem Beispiel sind zwei Signaturen auf einem Dokument angebracht. Der Validator prüft nun folgende mandantenspezifische Punkte:

1. Sind die Signaturen der unterschreibenden Parteien und der Urkundsperson (vorletzte Signatur) vom Typ qualifiziert (seit 2017 ist der qualifizierte Zeitstempel erforderlich, vor 2017 war der Zeitstempel optional).
2. Ist die Signatur der Zulassungsbestätigung (letzte Signatur) mit einem Signaturzertifikat von UPReg erstellt worden.
3. Stimmen die Claimed Attributes der UPReg-Zulassungsbestätigung mit den Werten der Signatur der Urkundsperson überein.

Die kryptografischen Prüfungen der Signatur (Prüfungen auf Unveränderheit, Zeitstempel-validierungen, Revokationschecks etc.) müssen unabhängig davon durchgeführt werden.