Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Technische Beschreibung der Zulassungsbestätigungssignatur

Auftraggeber	Bruno Frutiger (ISB)
Serviceverantw.	Peter Erz (ISB)
Autor	Igor Metz / Adrian Greiler (Glue)
Klassifizierung	**Nicht klassifiziert**
Status	**Genehmigt**

Änderungsverzeichnis

Datum	Version	Änderung	Autor
26.09.2018	0.1	Erste Fassung (auf Basis der Spezifikation von UPReg)	Glue
19.10.2018	0.9	Feedback des BJ aufgenommen	Glue
24.10.2018	1.0	Freigabe ISB	ISB

Inhaltsverzeichnis

1 Einleitung

Das Urkundspersonenregister (UPReg) bestätigt die Zulassung einer Urkundsperson mit einer zusätzlichen Signatur auf einem qualifiziert signierten Dokument. Diese zusätzliche Signatur wird mittels eines Programms, beispielsweise mit dem Open eGov LocalSigner oder durch Software von Drittanbietern im Zusammenspiel mit einem Webservice des UPReg angebracht (vgl. dazu Art. 9 EÖBV-EJPD [SR 211.435.11]). Dabei prüft UPReg die Signatur der Urkundsperson (erste Signatur) und signiert seinerseits das Dokument (zweite Signatur) erneut, um die Zulassung der Urkundsperson zu bestätigen.

Der Ablauf zur Erstellung einer elektronischen öffentlichen Urkunde gemäss EÖBV (SR 211.435.1) lässt sich grob und unter beispielhafter Einsetzung des LocalSigners wie folgt zusammenfassen (für Details siehe [1]):

1. Die Urkundsperson signiert ein PDF Dokument (qualifizierte Signatur).
2. Die Urkundsperson fordert mit LocalSigner die Zulassungsbestätigung für das qualifiziert signierte Dokument an. Dazu übermittelt LocalSigner in einem ersten Schritt die Signatur (als PKCS#7-Struktur) und den Hash des signierten Dokumentes an UPReg. UPReg prüft die Berechtigung anhand des Zertifikats in der qualifizierten Signatur.
3. LocalSigner errechnet den zu signierenden Hash des (qualifiziert signierten) PDF und übermittelt in einem zweiten Schritt den Hash an UPReg.
4. UPReg signiert den Hash und gibt die Signatur der Zulassungsbestätigung dem LocalSigner als PKCS#7-Struktur zurück.
5. LocalSigner bettet die Signatur von UPReg in das Dokument ein.

Da UPReg aus Gründen der Vertraulichkeit den Inhalt des jeweils im ersten Schritt signierten Dokument nicht einsehen kann, wäre es einer für den Zweck der Fälschung erstellten Software theoretisch möglich, im zweiten Schritt an UPReg den Hash eines anderen Dokuments zu senden und anschliessend die Zulassungsbestätigungssignatur in dieses Dokument einzufügen. Durch diese Manipulation könnte also ein Dokument entstehen, das als erste Signatur nicht die Signatur einer Urkundsperson trägt, aber trotzdem mit einer Zulassungsbestätigung versehen ist.

Um zu prüfen, ob ein Dokument eine gültige elektronische öffentliche Urkunde gemäss EÖBV ist, reicht es also nicht, nur die beiden Signaturen auf Gültigkeit zu prüfen.

Um Fälschungen erkennbar zu machen fügt UPReg in der zweiten Signatur immer einen Bezug auf das mit der ersten Signatur signierte Dokument ein. Die für den Bezug erforderlichen Informationen werden als sogenannte CMS Signed Attributes in die zweite Signatur eingebettet und sind somit gegen Verfälschung gesichert.

2 Referenzen

[1] Anhang 3 der Verordnung des Eidgenössischen Justiz- und Polizeidepartements (EJPD) über die Erstellung elektronischer öffentlicher Urkunden und elektronischer Beglaubigungen (EÖBV-EJPD; SR 211.435.11). Technische Anforderungen zur Vermittlung des Zugriffs auf das UPReg. Der Anhang kann unter www.bj.admin.ch > Wirtschaft > Elektronische öffentliche Urkunden und elektronische Beglaubigungen konsultiert werden.

3 CMS Signed Attributes in Zulassungsbestätigung

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.

3.1 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.

3.2 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), die von der Methode „rt1-generate“ (RT1) des REST Interfaces des Webservice Funktionsnachweis zurückgegeben wurde.
`2.25.155567022322770787173630853582050149659.2`	Timestamp der Anfrage (Unix-Time in Millisekunden).
`2.25.155567022322770787173630853582050149659.3`	UPReg-Domain, für welche diese Zulassungsbestätigung ausgestellt wurde. Entspricht dem JSON-Attribut domain beim Aufruf der der Methode „rt1-generate“ (RT1) des REST Interfaces des Webservice für die Zulassungsbestätigung.

OID	Beschreibung
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 der Methode „rt1-generate“ (RT1) des REST Interfaces des Webservice 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 der Methode „rt1-generate“ (RT1) des REST Interfaces des Webservice 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 der Methode „rt1-generate“ (RT1) des REST Interfaces des Webservice für die Zulassungsbestätigung extrahiert. Im Attribut pkcs7 ist die Signatur der Urkundsperson enthalten.
2.25.155567022322770787173630853582050149659.7	Kürzel des Kantons, für welchen diese Zulassungsbestätigung ausgestellt wurde. Entspricht dem JSON Attribut canton beim Aufruf der der Methode „rt1-generate“ (RT1) des REST Interfaces des Webservice für die Zulassungsbestätigung.

3.3 Struktur der Signed Attributes unter 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
```

Natürlich werden auch andere Werte für die Signatur gesetzt. Das folgende Beispiel zeigt alle von UPReg gesetzten Werte der Signatur für die Zulassungsbestätigung.

```
├1
│└2
│ └840
│    └113549
│           └1
│            └9
│             ├3   Content Type
│             └4   Message Digest
└2
 ├16
 │ └840
 │    └1
 │     └101
 │        └3
 │         └4
 │          └2
 │           └1   Message Digest Type SHA-256
 └25
   └155567022322770787173630853582050149659
                                              ├1   Transaktions-ID
                                              ├2   Timestamp
                                              ├3   UPReg-Domain
                                              ├4   X509-Issuer
                                              ├5   X509-Subject
                                              ├6   X509-Serial
                                              └7   Kantonskürzel
```

3.4 Beispiel möglicher Werte in CMS Signed Attributes

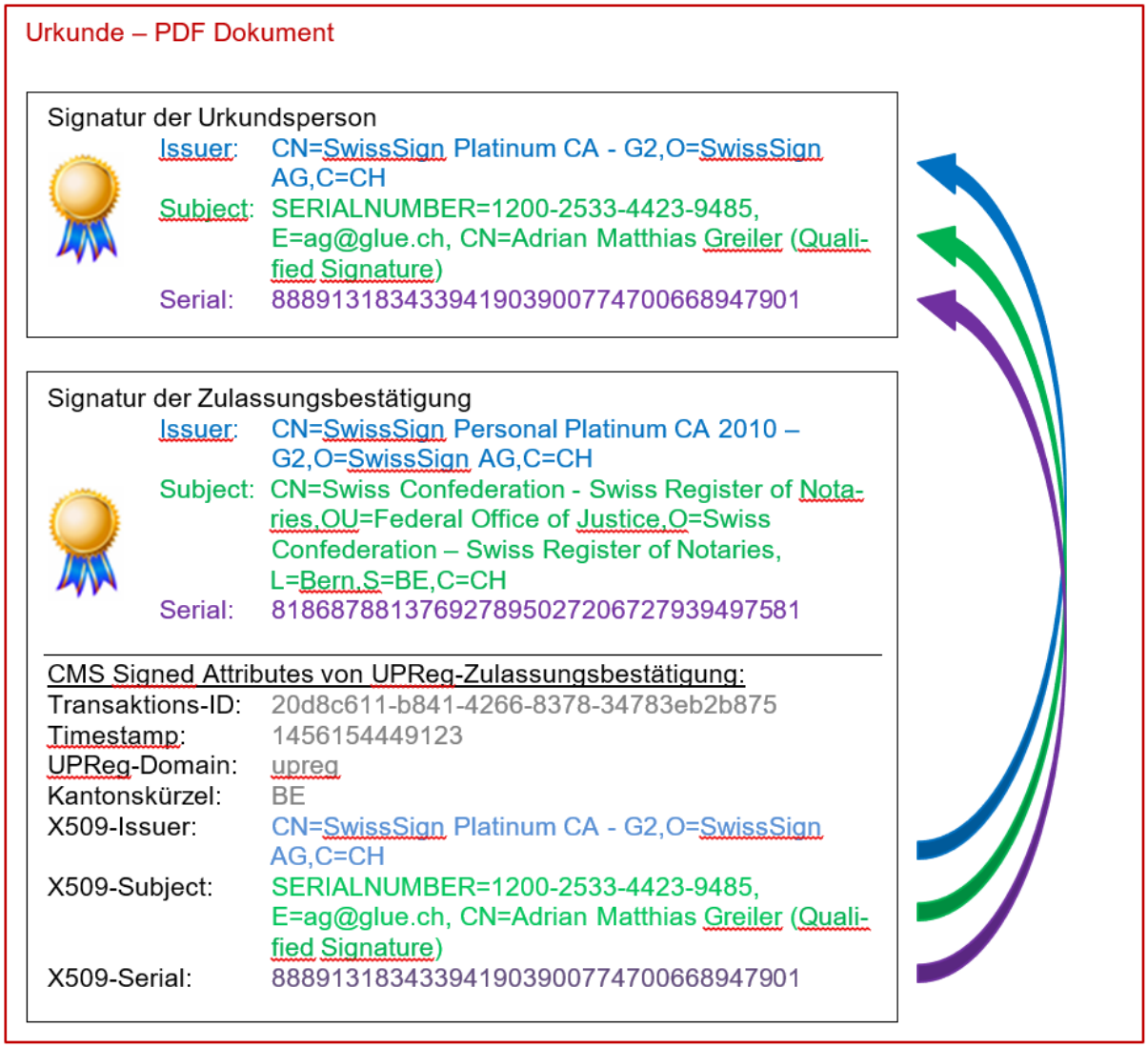
Beispiele für die Werte, welche für die Validierung der Signatur verwendet werden:

- 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 (Authentication)
- X509-Serial: 888913183433941903900774700668947901
- Kantonskürzel: BE

Die ersten drei Werte sind dabei lediglich Zusatzinformationen, welche dazu dienen, bei einem Supportfall oder einer Fälschung schneller den dazugehörigen Logeintrag in UPReg zu finden. Die drei Werte mit 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, muss von einer Fälschung ausgegangen werden.

3.5 Beispiel der Signaturen und CMS Signed Attributes auf dem Dokument

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



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

1. Ist die Signatur der Urkundsperson (erste / vorletzte Signatur) vom Typ «qualifiziert».
2. Ist die Signatur der Zulassungsbestätigung (letzte Signatur) mit dem Siegel von UPReg erstellt worden.
3. Stimmen die CMS Signed Attributes der UPReg-Zulassungsbestätigung mit den Werten der Signatur der Urkundsperson überein.

Die Prüfungen der Signatur sowie die Prüfungen auf Unveränderheit, Zeitstempelvalidierungen, Revokationschecks usw. werden wie gewohnt durchgeführt.