swisscom

C1 - Public

Fragen zum All-in Signing Service von Swisscom

Inhalt

1 Identifikation allgemein

(1) Sind Identifikationen auch für fortgeschrittene Signaturen längstens nur 5 Jahre gültig?

Ja nach 5 Jahren müssen auch für fortgeschrittene Signaturen identifizierte Personen neu identifiziert werden. Allerdings reicht es bei fortgeschrittenen Signaturen aus, wenn zum Zeitpunkt der Antragstellung der Ausweis gültig war. Läuft dieser binnen der 5 Jahre ab, ist keine Neuidentifizierung notwendig. Bei qualifizierten Signaturen ist eine Identifizierung hingegen längstens so lange gültig, wie der Ausweis gültig war oder bis maximal 5 Jahre nach dieser Identifizierung.

(2) Kann ich mich auch bei der Post, Swisscom Shops etc. identifizieren?

In der Schweiz ist Swisscom dabei, eine Identifikationsmöglichkeit auch in Shops der Swisscom zu ermöglichen. Allerdings sind hier vor Ende 2019 keine Möglichkeiten zu erwarten. Im Ausland wird es Identifikationen nur über Partner geben, die das anbieten. Mittelfristig sucht Swisscom die Anbindung an bestehende Identitäten (z.B. Identitätsfeststellung online durch eine Bank oder eine staatliche eID). In Q2 werden hier erste Projekte in Deutschland starten.

(3) Muss ich bei der Signaturanfrage genau die Identifikationsdaten nutzen?

Ja. Sofern im Signaturzertifikat genau der Name erscheinen soll, wie im Ausweisdokument, muss auch die Anfrage den genauen Namen mit allen Zunamen wie im amtlichen Dokument enthalten. Swisscom kann den Dienst aber auch so konfigurieren, dass anstelle des Namens im Zertifikat die Mobilnummer als Pseudonym genommen wird. Es steht dann weiterhin dem Anwender frei im "Common Name" (CN) den gewöhnlichen Vor- und Zunamen (unabhängig vom Ausweisdokument) zu nutzen. Der RA-Service

VerifyCall verifiziert in diesem Falle nur die Mobilnummer, die während der Identifikation angegeben wurde und das Heimatland gemäss Ausweisdokument.

2 PDF-Handling, Erzeugung Hash, Einbinden signierter Hash

(4) Gibt es Bibliotheken, die das Handling mit PDFs erleichtern?

Ja, auf dem Markt sind verschiedene Libraries vorhanden, die eine schnelle Implementierung einer Teilnehmerapplikation ermöglichen. Alle haben speziell auch für den Swisscom Service einen besonderen Support:

- *Fa. Intarsys, Deutschland*: stellt verschiedene Lösungen zur Verfügung zum Handling und Einbindung von Signaturen: https://www.intarsys.de/produkte/fernsignatur
  Intarsys ist Premium-Partner der Swisscom und kennt technisch den AIS Service sehr gut und kann hier im Consulting unterstützen.
- *Fa. PDF-Tools, Schweiz*: 3-Heights PDF Suite. http://www.pdf-tools.com/pdf20/de/produkte/pdf-security-signature/pdf-security/
- *iText, Belgien:* iTextPDF. https://itextpdf.com/de/products/product-tour. Swisscom nutzt in seinen Beispielen iText, allerdings sind die Beispiele "out of date", d.h. einige Funktionalitäten haben sich geändert. Aber das prinzipielle Handling ist dort ersichtlich: https://github.com/SCS-CBU-CED-IAM/itext-ais
- *Setasign, Deutschland:* Einige Kunden setzen SetaPDF ein, welche spezielle Lösung auch für den Swisscom Service bietet: https://www.setasign.com/products/setapdf-signer/demos/swisscom-all-in-signing-service/
- *Blocksigner, Schweiz (Skribble.com):* https://api.skribble.com/swagger-ui.html, http://doc.skribble.com/

Grundsätzlich lehnt Swisscom jegliche Verantwortung für das Funktionieren dieser Libraries ab. Diese können Fehler enthalten und bedürfen besonderes Wissen und Fachkenntnisse. Die Verwendung geschieht auf eigene Verantwortung durch den Teilnehmer.

(5) Wieviel Platz benötigt eine Signatur im Dokument?

Ca. 50 kBytes.

3 Leistungsfähigkeit

(6) Wieviele Signaturanfragen pro Minute verkraftet unser System derzeit?

Im Moment sind wir dabei die Kapazitäten durch andere Algorithmen (Vorerzeugung von Schlüsseln) und HW Ausbau stark auszubauen. Da mehrere Kunden den Service nutzen gehen wir pro Kunde durchschnittlich von einer Maximallast von einer Anfrage pro Sekunde aus. Höhere Performance, d.h. besonders reservierte Kapazitäten sind optional möglich.

4 Multiple Signaturen

(7) Können auch mehrere Signaturen auf einem Dokument platziert werden?

Ja, das ist alleinige Aufgabe der Teilnehmerapplikation, die dann immer wieder den Hash mit dem Signaturwunsch zum All-in Signing Service sendet. Es können damit beliebig viele Signaturen für das digitale Dokument erzeugt werden.

(8) Kann ein Dokument mit einer Organisationssignatur (static signature) und einer Personensignatur (on-demand) versehen werden?

Ja, aber das verlangt 2 Kommunikationskanäle und Setups, d.h. die Signatur muss zunächst authentisiert durch den Signierenden über den einen Kanal personensigniert werden (on Demand) und dann geschützt durch ein SSL Authentisierungszertifikat über einen zweiten Kanal organisationssignert (mit zuvor angelegtem statischen Zertifikat).

(9) Wie wird eine Bulksignatur abgerechnet, d.h. in einer Signaturanfrage sende ich z.B. 5 Dokumente?

Jede Signatur wird einzeln berechnet, d.h. in diesem Beispiel werden 5 Signaturen abgerechnet.

(10) Wieviele Dokumente können mit einer Bulksignatur maximal mitgegeben werden?

Ca. 250. Die Beschränkung ergibt sich weniger aus dem Service als aus den Security Systemen.

(11) Können über eine Anbindung (ClaimedIdentity) sowohl fortgeschrittene als auch qualifizierte Signaturen ausgestellt werden?

Ja das ist möglich und wird im Rahmen der Anfrage im Protokoll geregelt.

5 RA-App

(12) Wie kann ich mit der RA-App testen?

Es gibt einen Test- und Demomode, mit dem man die App ausprobieren kann, bei der aber keine Daten übermittelt werden. Hierzu muss in der Anmeldung die Mobilfunknummer +41001234567 eingegeben werden und als Firmenbezeichnung "demo".

(13) Welche Länder unterstützt die RA-App?
Nachfolgend ist eine Auflistung der unterstützten Ausweisdokumente aufgeführt:

Land	Pass	ID
Afghanistan	✓	
Ägypten	✓	
Albanien	✓	
Algerien	✓	
Andorra	✓	
Angola	✓	
Argentina	✓	
Armenien	✓	
Äthiopien	✓	
Australien	✓	
Bangladesh	✓	
Belgien	✓	✓
Benin	✓	

Bosnien & Herzegowina	✓	
Botswana	✓	
Brasilien	✓	
Bulgarien	✓	✓
Chile	✓	
China	✓	
Costa Rica	✓	
Dänemark	✓	
Deutschland	✓	✓
Dominikanische Republik	✓	
Ecuador	✓	
Elfenbeinküste	✓	

Eritrea	✓	
Estland	✓	✓
Finnland	✓	✓
Frankreich	✓	✓
Georgien	✓	
Ghana	✓	
Großbritannien	✓	
Griechenland	✓	✓
Haiti	✓	
Indien	✓	
Irak	✓	
Iran	✓	
Irland	✓	
Island	✓	

Israel	✓	
Italien	✓	✓
Jamaika	✓	
Japan	✓	
Jordanien	✓	
Kamerun	✓	✓
Kanada	✓	
Kasachstan	✓	
Katar	✓	
Kolumbien	✓	
Kongo	✓	✓
Kosovo	✓	✓
Kroatien	✓	✓
Kuba	✓	
Laos	✓	
Lettland	✓	✓
Libanon	✓	
Liechtenstein	✓	✓
Litauen	✓	✓
Luxemburg	✓	✓
Malaysia	✓	
Marokko	✓	
Mazedonien	✓	
Mexiko	✓	
Moldau	✓	
Montenegro	✓	
Mosambik	✓	
Namibia	✓	
Neuseeland	✓	✓
Niederlande	✓	✓
Nigeria	✓	
Norwegen	✓	
Österreich	✓	✓
Pakistan	✓	
Peru	✓	
Philippinen	✓	
Polen	✓	✓
Portugal	✓	✓
Rumänien	✓	✓
Russland	✓	
Schweiz	✓	✓
Schweden	✓	✓
Senegal	✓	
Serbien	✓	

Singapore	✓	
Slowakei	✓	✓
Slowenien	✓	✓
Somalia	✓	
Spanien	✓	✓
Südafrika	✓	
Südkorea	✓	
Syrien	✓	✓
Thailand	✓	✓
Togo	✓	
Tschechische Republik	✓	✓
Tunesien	✓	✓
Türkei	✓	
Uganda	✓	
Ukraine	✓	
Ungarn	✓	✓
Uruguay	✓	
USA	✓	
Venezuela	✓	
Vietnam	✓	

(14) Muss der RA Agent von Swisscom beauftragt werden, wenn er Personen für Signaturen nach EU und CH Gesetz identifiziert?

Indirekt geschieht das. Praktisch ist der Ablauf folgender: Die RA Agentur ernennt zuerst einen RA-Master Agenten. Dieser wird von Swisscom oder einem Swisscom Partner identifiziert und durchläuft eine Schulung. Anschliessend erhält er eine Bedienoberfläche mit der er weitere alleinig von ihm identifizierte Personen zu RA-Agenten oder RA-Master Agenten machen kann. Diese müssen aber ebenfalls eine Schulung durchlaufen.

(15) Wie wird eine Person aus dem RA-Service wieder gelöscht?

Grundsätzlich muss Swisscom die Daten bei geleisteter Signatur sehr lange (11 Jahre in der Schweiz oder 35 Jahre in der EU) behalten. Aber Personen können vom RA-Master Agenten oder von der Swisscom inaktiv gesetzt werden, so dass diese nicht mehr signieren können.

(16) Werden die Daten von EU berechtigten und CH berechtigten Signierenden getrennt gehalten?

Ja, es wird unterschieden, ob die Signierenden zu den Nutzungsbedingungen der Schweiz oder der EU oder beiden zugestimmt haben. Alle Daten werden von der Swisscom (Schweiz) AG auch für die Swisscom IT Services Finance S.E. in Wien verarbeitet.

(17) Wie lange benötigt ein trainierter RA-Agent für eine Identifizierung?

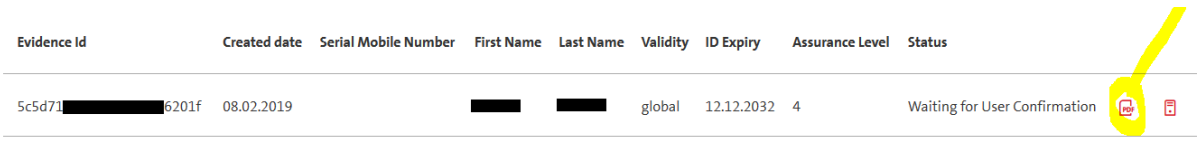
Im Durchschnitt wird eine Identifizierung binnen 2 Minuten abgeschlossen.

(18) Beim Fotografieren der Vorder-/Rückseite des Ausweises fokussiert die Kamera nicht...

Halten Sie die Kamera so hoch, dass das komplette Ausweisdokument vom Ausschnitt (ggfs. noch unscharf) erfasst wird. Führen Sie die Kamera langsam an den Ausweis näher, er fängt dann wieder an zu fokussieren.

(19) Die registrierte Person hat die SMS nicht erhalten oder gelöscht mit der Akzeptanz der Nutzungsbestimmungen

Benachrichtigen Sie Ihren RA-Master Agenten und bitten ihn im Portal nach der Mobilnummer zu suchen. Sie können die SMS mit den Nutzungsbestimmungen erneut aussenden durch Betätigen des Links mit dem PDF Symbol:



Evidence Id	Created date	Serial Mobile Number	First Name	Last Name	Validity	ID Expiry	Assurance Level	Status
5c5d71[redacted]6201f	08.02.2019		[redacted]	[redacted]	global	12.12.2032	4	Waiting for User Confirmation

(20) Die registrierte Person hat keine SMS erhalten und ist nicht auffindbar

Stellen Sie sicher, dass Sie die Person nicht im RA-App Demo Mode (Mobilnummer +41001234567, Firma "demo") registriert haben.

6 Authentisierungsmethoden Mobile ID und SMS

(21) Ist für die Authentifizierung nur Mobile ID oder PWD/OTP möglich?

In der Schweiz schalten wir standardmässig Mobile ID auf mit einem automatischen Rückfall auf PWD/OTP, falls die SIM Karte nicht für Mobile ID freigeschaltet ist. Im eIDAS Raum lassen wir standardmässig nur PWD/OTP zu.

Ab ca. Q1 2020 werden wir auf Basis der Mobile ID Schnittstelle eine Authentifizierungsapp anbieten, die auch Authentifizierungen mit Fingerprint oder Face Recognition anbietet. Diese App benötigt während der Authentifizierung nur eine Internetverbindung und kann damit international eingesetzt werden. Eine internationale SIM Karte (Mobilfunknummer) ist aber weiterhin notwendig für das Setup der App. Siehe http://documents.swisscom.com/product/filestore/lib/0027a527-304d-44a3-b467-9e655ee7025e/mobileidapp-en.mov.

Generell sind auch andere Authentifizierungsmethoden möglich, diese müssen aber von KPMG zugelassen werden. Das müsste der Partner machen und seine Methode im Rahmen eines Umsetzungskonzeptes zeigen.

(22) Ich wurde mit PWD/OTP identifiziert und habe nun eine MobileID, kann ich damit signieren?

Nein. Sie haben damit ein neues Authentifizierungsmittel, welches initial nicht mit der Identifikation erfasst wurde. D.h. Sie müssen sich neu identifizieren lassen unter Nutzung der MobileID.

(23) Ist ein Mobilfunkempfang via SMS auch im Ausland sichergestellt?

Keine Garantie, aber es sollte in fast allen Fällen funktionieren – man kann sich an dieser Auskunft orientieren:

https://www.swisscom.ch/en/residential/mobile/tariffs-roaming-abroad/query-tariffs.html

Voraussichtlich in Q4/2019 werden wir die Authentifizierung um weitere Faktoren erweitern (Authentifizierungs-App). Bis dahin kann aufgrund des Fremdproviders im Ausland Swisscom keine Garantie geben über die Authentifizierungsmöglichkeit im Ausland.

(24) Ist ein Mobile ID Empfang auch im Ausland sichergestellt?

Mobile ID wird auch überall im Ausland empfangen – überall dort, wo eine SMS empfangen werden kann, Es läuft über ein Sonderprotokoll im Telekommunikationsstandard. Da viele externe Parteien in den Empfang involviert sind, kann Swisscom einen Empfang der MobileID nicht garantieren.

(25) Wofür benötigte es auch noch ein Password und die SMS reicht nicht für eine qualifizierte Signatur?

Für die qualifizierte Signatur ist eine 2-Faktor Authentisierung vorgeschrieben: "Besitz" und "Wissen", d.h. nur der Besitz (SMS) reicht nicht.

(26) Ist 2FA Autorisierung auch für fortgeschrittene Signaturen notwendig?

Nein, für fortgeschrittene Signatur reicht OTP.

(27) Entstehen bei der Mobile ID oder der SMS Kosten?

Swisscom berechnet keine Kosten beim Versand der Mobile ID oder SMS. Allenfalls im Roaming können je nach Tarif des Roaming Partners ggfs. Kosten anfallen.

(28) Was passiert wenn ich mein Passwort vergessen haben?

Der Verlust des Passworts führt zu einer neuen digitalen Identität. Die Applikationsanbieter können darauf reagieren und ggf. eine neue Identifikation des Signierenden verlangen, z.B. mit der RA-App.

(29) Was passiert bei einer Rufübernahme durch eine andere Person?

Da beiden Methoden sowohl neben dem Besitz der Rufnummer auch die Eingabe ein Geheimnis verlangen, kann nach Übernahme der Rufnummer keine Signatur für die vorgängig bestehende digitale Identität ausgelöst werden. D.h. die Person muss neu identifiziert werden.

(30) Kann auch ein Festnetztelefon anstelle eines Mobiltelefons für die SMS Abfrage genutzt werden?

Da eine Festnetznummer praktisch nicht einer Person zugeordnet werden kann, ist das nicht möglich. Mit der SMS soll ja sichergestellt werden, etwas zu erreichen, was alleinig und ohne Ausnahme der signierenden Person zugeordnet ist.

(31) Kann man auch ohne Mobilfunkempfang signieren?

Moderne Geräte verfügen über WIFIcalling. Mit diesen kann auch in einer WIFI Zone signiert werden. Ohne Internet ist hingegen keine Fernsignatur möglich.

(32) Wird MobileID via eSIM unterstützt?

In der Regel ja.

(33) Was passiert, wenn ich die SIM Karte wechsle?

Im Falle einer MobileID können Sie mit einem Wiederherstellungscode die MobileID auf die neue SIM übertragen. Im Falle von PWD/OTP und gleicher Rufnummer bleibt ebenfalls Ihre Möglichkeit zur Authentifikation bestehen.

(34) Wie geschieht die Verknüpfung der Identifikation mit einer Authentisierungsmethode?

Bei der Identifizierung wird das Authentisierungsmittel (z.B. konkret die Mobilfunknummer) abgefragt. Mit dieser wird bereits eine erste Signatur durchgeführt, typischerweise die Signatur der Nutzungsbestimmungen, die akzeptiert wurden. Diese Signatur wird zum All-in Signing Service übertragen. Damit kennt das All-in Signing System genau das Authentisierungsmittel.

(35) Gibt es eine API anstelle der Einbindung des Password/OTP Screens?

Nein. Swisscom hat sogar die Auflage, bei der Einbindung des PWD/OTP Screens als "iFrame" eine Möglichkeit zu geben, dass eine externe Person prüfen kann, dass diese von Swisscom stammt. Hier können z.B. die Standard Browser Funktionen genutzt werden, die Swisscom unter seinem Webseitenlink gemäss Kapitel 4 der Nutzungsbestimmungen publiziert.

(36) Kann ich Screen Scrapping für OTP/PWD Eingabe einsetzen?

Screen Scrapping wird als Interface nicht unterstützt. Entwickler müssen damit rechnen, dass die Screens verändert werden. Zudem widerspricht es dem "Sole Control" Gedanken des direkten Zugriffs des Signierenden auf das Unterschriftenzertifikat.

(37) Kann der Password/OTP Screen eingebunden werden in eine Webseite/Applikation?

Ja. Allerdings nur als iFrame, siehe Anleitung unter https://rasp.scapp.swisscom.com/swagger-ui.html .

(38) Kann der Password/OTP Screentext oder MobileID Text konfiguriert werden?

Ja. Im Rahmen des Protokolls kann, wie im Reference Guide (www.swisscom.com/signing-service) unter "Step-Up Methode" beschrieben, im "Message" Feld der Textblock mit der Überschrift zur Nachricht für die Willensbekundung und mit "Language" die Spracheinstellung konfiguriert werden. Für das SMS Eingabefenster kann ebenfalls die Sprache mit dem "Language" Parameter eingestellt werden.

(39) Was passiert, wenn MobileID auf einer SIM Karte nicht aktiviert oder möglich ist?

MobileID wird immer in Kombination mit einer Rückfalllösung PWD/OTP konfiguriert, d.h. es wird automatisch ein Passwortfenster gesendet. Eine MobileID kann unter https://mobileid.ch aktiviert werden.

(40) Wann wird das Passwort erstmalig festgelegt?

Im Standardfall erhält der Kunde nach der Identifikation zunächst die Nutzungsbestimmungen zum Signaturservice der Swisscom. Diese bestätigt er und löst damit eine erstmalige Signatur dieser Bedingungen aus, in dessen Kontext er auch erstmalig das Passwort festlegen kann.

(41) Können anstelle von PWD/OTP – MobileID auch weitere Authentisierungsmethoden genutzt werden?

Standardmässig werden von Seiten Swisscom im Moment nur diese Methoden angeboten. Das Angebot wird aber in Zukunft ausgearbeitet, so dass – sofern die Zulassung vorliegt – auch biometrische Methoden möglich sein können. Des weiteren begleitet Swisscom optional auch den Kunden, falls dieser mit einer auditierten Lösung bei der Anerkennungsstelle eine weitere Signatur zulassen möchte. Hierbei fallen weitere Kosten an.

(42) Reicht als 2-Faktor Lösung nicht ein Login bei der Teilnehmerapplikation und eine SMS aus?

Basis der 2-Faktor Authentisierung ist die Tatsache, dass beide Faktoren im Zusammenhang mit der Authentisierung erfasst werden müssen, d.h. es darf dann kein Passwort gewählt werden, welches nur die Teilnehmerapplikation kennt, der Teilnehmer selber wurde aber mit RA-App identifiziert. D.h. so ein Ausnahmetatbestand könnte man sich höchstens vorstellen, wenn der Teilnehmer selber eine freigegebene Identifikation per RA-Delegation durchführt und darüber hinaus das Authentisierungsverfahren so gestaltet, dass in einer kurzen Session beide Faktoren (Login, SMS-Freigabe) durchgeführt werden. Sowohl das eigene Identifikationsverfahren als auch dieser Session Ablauf ist in einem Umsetzungskonzept detailliert zu beschreiben und benötigt eine Freigabe. Es fallen hier zusätzliche Kosten an.

(43) Sind Stapelsignaturen möglich?

Ja, mit einer Freigabe können mehrere Dokumente signiert werden.

(44) Sind XADES (XML) Signaturen möglich?

Mit Siegeln können XML Signaturen nach dem XADES Standard durchgeführt werden. Clientseitig muss der XADES Standard vorbereitet werden. Hierzu ist in der Implementierung der Aufruf der "plain signature" zu beachten. Personensignaturen nach dem XML Standard sind vorerst (noch) nicht möglich.

5.1.5.1 Signature Type

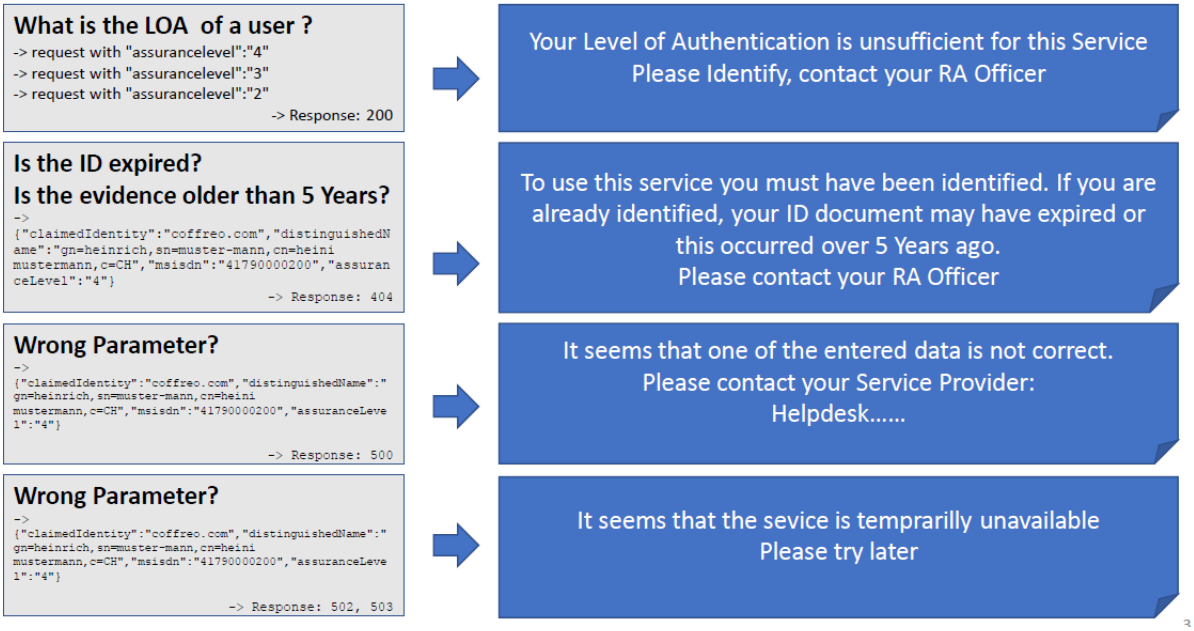
The element <SignatureType> defines the type of signature to be applied to the hash. There are currently three types of signature provided by AIS. Exactly one type of the following URN must be given in the request:

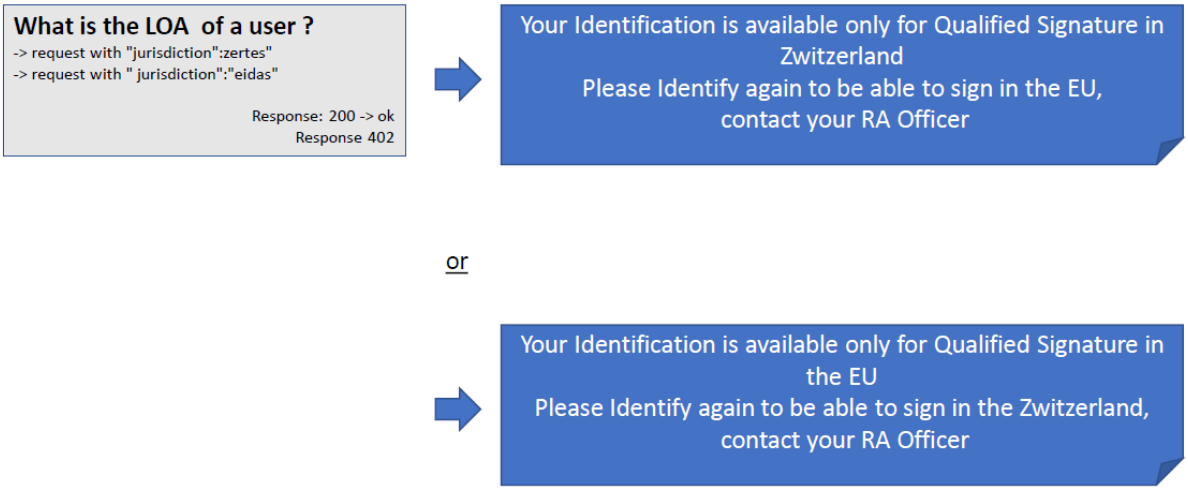
- **urn:ietf:rfc:3161**
  Creation of a Trusted Timestamp according to [RFC3161]. The response contains a Base64 encoded timestamp token. Optionally it may contain additional **revocation information** (chapter 5.1.5.5).

- **urn:ietf:rfc:3369**
  Creation of a CMS Signature according to [RFC5652]. The response contains a Base64 encoded signature. Optionally it may contain additional embedded **revocation information** (chapter 5.1.5.5) and/or an additional **timestamp** (chapter 5.1.5.4).

- **urn:ietf:3447 (http://ais.swisscom.ch/1.1/signaturetype/plain)**
  Creation of a static plain signature in PKCS#1 format (according to [RFC3447]).

(45) Wie lassen sich die Fehlercodes beim RA-Service am besten interpretieren?





(46) Serial Number mismatch

Was bedeutet die Fehlermeldung: *"Serial Number Mismatch. We strongly advise to go through the Pre-Signing Process in order to retrieve the actual StepUp SerialNumber*". Diese Fehlermeldung deutet darauf hin, dass bei einem PWD/OTP Prozess das Passwort zurückgesetzt und neu gewählt wurde ohne eine neue Identifikation mit entsprechendem Step-up Process gemäss Reference Guide durchzuführen.

(47) Warum hat meine Signatur nicht funktioniert?

Ich habe korrekt mich mit PWD/OTP oder MobileID authentifiziert – dennoch funktionierte die Signatur nicht … was kann die Ursache sein?

Ursachen sind:

- Sie haben beim PWD/OTP Verfahren ein neues Passwort gesetzt. Das darf nur in Ausnahmesituationen bei einer internen Registrierungsstelle durchgeführt werden und muss sonst immer im Rahmen einer Neuidentifikation stattfinden.
- Sie hatten bisher mit PWD/OTP authentifiziert und haben nun mit einer Schweizer Mobilfunknummer ihre MobileID freigeschaltet. In diesem Fall muss auch eine Neuidentifikation stattfinden, da sich das zur Identität gehörende Authentifizierungsmittel geändert hat.
- Sie haben die SIM gewechselt, bzw. den Mobilfunkprovider. Dadurch hat sich bei einem MobileID Einsatz die MobileID Authentifizierung geändert. Hierfür ist ebenfalls eine Neuidentifikation notwendig
- Liegt keiner dieser Ursachen vor, sollten Sie ein Ticket eröffnen.

7 Validierung der Signatur

(48) Wie kann ich Signaturen validieren lassen?

Für Signaturen im Rechtsraum Schweiz: www.validator.ch (Achtung, der Validator entspricht nicht immer dem neuesten Stand). Für Signaturen im Rechtsraum EU: https://www.signatur.rtr.at/de/vd/Pruefung.html

(49) Wieso zeigt der Validator eine ungültige Signatur an?

Häufig beziehen sich die Meldungen auf die fehlende Integrität, d.h. das Dokument weist Änderungen nach Setzen der Signatur auf. Z.B. wurden Elemente aus dem Netz nachträglich noch eingesetzt. Das kann vermieden werden, indem konsequent der PDF/A Standard letzter Ausprägung zur Signatur verwendet wird.

(50) Zeigt der "grüne Haken" in Adobe die Gesetzmässigkeit der Signatur an?

Adobe ist ein U.S. amerikanischer Hersteller unter anderem von Software, die PDF Dokumente anzeigen kann. Prominentestes und weit verbreitetes Produkt ist der sogenannte "Adobe Acrobat Reader". Dieser ermöglicht die Überprüfung von zertifikatsbasierten Signaturen. Ob eine Signatur gültig und damit mit grünem Haken angezeigt wird, richtet sich nach vielen Gesichtspunkten:

- Adobe führt ein eigenes Regelwerk, nachdem es prinzipiell herausgebende CAs von Vertrauensanbietern oder Zerifizierungsdienstleistern als "vertrauenswürdig" einstuft. Diese werden in einer sogenannten Adobe Trust List (AATL) geführt. Auch wenn nicht in der Leistungsbeschreibung enthalten, bemüht sich Swisscom immer darum, hier aufgeführt zu sein. Das Regelwerk richtet sich nicht nach rechtlichen Vorgaben, sondern nach Konzernvorgaben, hinzu kommt, dass die aufgeführten Unternehmen hierfür auch jährliches Geld zahlen müssen. Für die Erfüllung der Regeln müssen sie ein Self-Assessment durchführen. eIDAS Vertrauensdiensteanbieter werden nach Aussage des Konzerns wohl als vertrauenswürdig geführt, sofern sie auch einen Vertrag mit Adobe abgeschlossen haben.
- Adobe bietet viele Einstellmöglichkeiten, die dazu führen, dass die Prüfung nach ganz anderen Gesichtspunkten erfolgt: Beispielsweise kann anstelle der Vertrauensliste von Adobe auch die Vertrauensliste von Microsoft Windows herangezogen werden, die in der Regel aber nur Vertrauensdiensteanbieter führt, die auch SSL oder E-Mail Zertifikate herausgeben. Gleichwohl kann die Prüfung auch anhand eines Zeitpunktes erfolgen, der durch die Computeruhr gegeben ist und nicht anhand des im Dokument geführten Zeitstempels.

D.h. somit kann man sich auf die Gültigkeit einer Unterschrift in Adobe nicht verlassen, hingegen bekommt man Informationen darüber, ob nach dem Setzen der Unterschrift noch Änderungen am Dokument stattgefunden haben und wie das Signaturzertifikat ausschaut.

8 Vertragsfragen

(51) Die Konfigurations- und Annahmeerklärung sieht die Benennung zweier Rollen vor: (1) Security Officer für Datensicherheit und Datenschutz (2) System Administrator. Wie habe ich diese Rollen passend zu wählen?

Beides sollten Personen aus der IT sein, die die Applikation kennen. Es muss nicht eine Person mit der offiziellen Rolle "Datenschutz" sein. Swisscom will hier einfach das 4-Augen Prinzip beibehalten. Die Rollen sind: Auskünfte geben können über die Administration der Benutzerapplikation (wer hat Zugang, was könnte ein Administrator manipulieren, wo hakt es ggfs., SSL Connection zu Swisscom) und beim Sicherheitsverantwortlichen Themen wie Virenschutz, Zugangskontrolle allgemein, etc.

(52) Was mache ich in einem Unternehmen mit mehreren Tochtergesellschaften?

Zum einen kann eine interne Gesellschaft "Reselling Partner" von Swisscom werden für andere Gesellschaften. Dann geht der Zahlungsfluss direkt nur über diese einzelne Gesellschaft. Es kann auch eine Gesellschaft die komplette Verantwortung für den Betrieb der Teilnehmerapplikation übernehmen. Auch

dann gehen Rechnungen nur über diese Gesellschaft. Sie kann dann Mitarbeiter der anderen Gesellschaften identifizieren.

Sofern alle Gesellschaften unabhängig die Teilnehmerapplikation betreiben wollen (mit jeweils eigener Haftung und Verantwortung) und auch selber RA-Agenten stellen wollen, bedarf es für jede Gesellschaft einen eigenen Vertrag.

(53) Wir möchten teilweise "per Signierenden" und teilweise "pro Signatur" abrechnen, geht das?

Hierbei müssen 2 Benutzeraccounts (ClaimedIdentity) eröffnet werden, jeder Account ist mit einer Abrechnungsmethode verbunden. Beide Accounts können über eine Schnittstelle, d.h. dem gleichen Endpunkt angesprochen werden. D.h. die Teilnehmerapplikation muss selber entscheiden, über welchen Account sie eine Signaturanfrage sendet. Pro Account fällt eine Servicegebühr an, allerdings verringert sich die Transaktionsgebühr pro Signatur um 30%. Es werden am Monatsende 2 Rechnungen ausgestellt. Es fallen daher die Servicegebühren im Vertrag doppelt an.

(54) Wenn "per Signierenden" abgerechnet wird, was passiert mit den Monaten in denen nicht signiert wird?

Hier fallen keine Kosten an.

(55) Wir möchten sowohl in der EU als auch im CH Rechtsraum signieren, geht das?

Hierbei müssen 2 Benutzeraccounts (ClaimedIdentity) eröffnet werden, jeder Account ist mit der jeweiligen Signaturart verbunden, d.h. die Teilnehmerapplikation muss entscheiden, über welchen Account sie eine Signaturanfrage sendet. Beide Accounts können über eine Schnittstelle, d.h. dem gleichen Endpunkt angesprochen werden. Pro Account fällt eine Servicegebühr an, allerdings verringert sich die Transaktionsgebühr pro Signatur um 30%. Es werden am Monatsende 2 Rechnungen ausgestellt. Es fallen daher die Servicegebühren im Vertrag doppelt an. Sofern man also 2 Rechtsräume und 2 Abrechungsarten hat, hat man weiterhin nur eine Schnittstelle (technisch), aber 4 Accounts und 4 SAIPs, d.h. die Servicegebühren fallen 4-fach an.

(56) Swisscom verwendet Standard PDF Verträge – wie können wir die anpassen?

Swisscom investiert jährlich hohe Summen in die fortwährenden Audits. Um dennoch das Angebot eines Trust Service Providers am Markt preisgünstig platzieren zu können, wird dieser Service in einer standardisierten Form angeboten. Es findet pro Kunde kein "Projekt" statt, sondern Signaturen werden als Plattformgeschäft verkauft. Das heisst insbesondere:

- Es ist der Standardprozess der Bestellung mit den durch die Auditoren mitgeprüften Vertragstexten einzuhalten.
- Weitere Assessments durch Teilnehmer und die Prüfung und Annahme eigener Vertragstexte sind im Angebot nicht inbegriffen.

Viele Aspekte des Trust Service Providers unterliegen nicht nur Auflagen in der Ausführung des Services sondern auch in der Festschreibung wichtiger Pflichten, Haftungsregelungen und Mitwirkungsleistungen in den Vertragsunterlagen. Daher unterliegen diese Vertragsunterlagen auch der Auditierung bzw. werden auch den staatlichen Konformitätsbewertungsstellen vorgelegt. Daher können weder Änderungen des Rechtssystems akzeptiert werden, noch vertragliche Beilagen des Teilnehmers insbesondere, wenn diese fremden, anwendbaren Recht unterliegen.

Ist es dennoch notwendig, vertragliche Texte anzupassen, vertragliche Regelungen hinzuzufügen (z.B. eigene Code of Conducts, Data Protection Declaration etc.), besondere Assessmentfragebögen zu

bearbeiten oder haben Sie gar Fehler oder unklare Formulierungen entdeckt, so melden sie diese bitte an unser Produktmanagement.

Sofern allfällige Fehler oder Unklarheiten ersichtlich sind, wird ein entsprechender Change Prozess seitens Produktmanagement hierzu angestossen und schnell möglichst umgesetzt.

Für die Bewertung anderer Fragen wird ein Bearbeitungsteam gebildet, dass die entsprechenden Experten (z.B. Rechtsabteilung, Sicherheitsverantwortlicher, Compliance Officer, etc.) heranzieht und eine Bewertung der Anfrage durchführt. Hierfür wird eine Bearbeitungsgebühr von CHF 6'000 fällig. Sofern das Expertenteam nicht direkt eine Lösung erarbeiten konnte, wird dieses eine Antwort und Angebot erarbeiten, welche weiteren Schritte seitens Swisscom vorstellt und abschätzt.

(57) Benötigt der Kunde Zertifizierungen für den Betrieb der Signaturapplikation?

Nein, nur für den Betrieb der Signaturapplikation benötigt es keine Zertifizierung und kein offizielles Audit mit Zertifikat. Der Kunde gibt im Rahmen einer "Konfigurations- und Annahmeerklärung" eine Selbstdeklaration ab, die Signaturapplikation ordnungsgemäss zu betreiben, d.h. z.B. den Hash eines Dokumentes nicht auszutauschen und dem Kunden das zu signierende Dokument auch tatsächlich anzuzeigen (WYSIWYS = "What you see is what you sign"). Auch der Datenverkehr sollte verschlüsselt zur Swisscom erfolgen und der Grundschutz in Bezug auf Viren und Angriffe sollte wie bei jedem anderen System gewährleistet sein. Nur eine eigene Identifikation insbesondere auch in Bezug mit einer eigenen Authentisierungsmethode kann ein Audit mit Zertifikat notwendig machen. In der Schweiz kann eine Identifikation mit Authentisierungsmethoden von Swisscom vereinfacht durch ein geeignetes vom Kunden vorgelegtes und von Swisscom abgenommenes "Umsetzungskonzept" abgehandelt werden, in der EU ist in der Regel ein Audit notwendig. Eine Authentisierungsmethode muss in der Regel immer zertifiziert werden, da hierdurch der "alleinige Zugriff" (im ETSI Kontext "Sole Control" genannt) sichergestellt werden sollte.

(58) Wie kann ich als Unternehmen Siegel bestellen?

Grundsätzlich muss das Unternehmen Vertreter benennen. Diese Vertreter sollten entweder die eingetragenen Vertreter gemäss Handels- oder Unternehmensregister sein, oder Vollmachten von diesen vorweisen können. Die Personen müssen in jedem Fall persönlich identifiziert werden mit unserer RA-App. In der Schweiz können nur im UID Register eingetragene Unternehmen Siegel bestellen. Beim Siegel dient das SSL Zugangszertifikat zwischen Signaturapplikation beim Kunden und Swisscom als Authentisierung des Unternehmens. Daher muss das Zugangszertifikat vom Vertreter der Organisation übergeben werden. Beim fortgeschrittenen Siegel reicht die einfache Zusendung, beim qualifizierten Siegel findet eine gemeinsame Übergabezeremonie statt, bei der das Zugangszertifikat gemeinsam erzeugt wird. Der private Schlüssel muss dabei auf einem Kryptodevice abgespeichert werden (FIPS 140-2 level 2 minimum).

(59) Wer haftet für fehlerhafte Zertifikate?

Grundsätzlich ist nach dem Gesetz Swisscom unbegrenzt haftbar für die Falschausstellung von qualifizierten Zertifikaten. Im Rahmen der fortgeschrittenen Zertifikate kann diese Haftung begrenzt werden. Swisscom schliesst hierfür auch entsprechende Pflichtversicherungen ab. Im Rahmen von Fehlern auf der Signaturapplikation (z.B. der Austausch eines Hashes eines Dokumentes) oder bei Fehlern bei der Identifikation durch dritte Registrierungsstellen, wird Swisscom seinerseits diese Dritte in Haftung nehmen. Um die Risiken einer Haftung zu vermeiden, werden an den Ausstellungs- und Vertragsprozess hohe Anforderungen gestellt und generell auch die Möglichkeit einer Auditierung der beteiligten Dritten gefordert.

9 Rechtswirkung einer Signatur

(60) Ist die Signatur in der Schweiz anerkannt?

Die schweizerische Gesetzgebung, d.h. das Schweizerische Bundesgesetz über die elektronische Signatur (ZertES), sieht die Einzelheiten vor, nachdem Unternehmer als Zertifizierungsdienst anerkannt sind. Die akkreditierte Anerkennungsstelle für die Anerkennung von Swisscom als Zertifizierungsdienst in der Schweiz ist die KPMG (Akkr. Nr. SCESm 0071). Sie stellt eine Konformitätsbewertungsbestätigung aus (zu finden unter www.swisscom.com/signing-service). Die Schweizerische Akkreditierungsstelle SAS führt eine Liste der akkreditierten Zertifizierungsdiensten:
https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas/pki.html

(61) Ist die Signatur in einem EU Land (auch ausserhalb von Österreich) anerkannt?

Mit dem Inkrafttreten der Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt der Europäischen Union (eIDAS) wurde die Basis für eine europaweite, rechtsgültige elektronische Kommunikation und sichere elektronische Identifizierung geschaffen. Mit Hilfe der Vertrauensdienste, wie elektronischen Signaturen, Siegeln, Zeitstempeln, Zustelldiensten und Zertifikaten zur Authentifizierung, können Unternehmen, Verwaltungen und Privatpersonen digitale Dokumente wie Angebote, Bestellungen, Verträge u.v.m. innerhalb der Europäischen Union auf einer einheitlichen Rechtsbasis austauschen. Damit löst die neue EU Verordnung das nationale Signaturgesetz und Signaturverordnungen ab.

Nach dieser EU-Verordnung (EU) Nr. 910/2014/EU (eIDAS-Verordnung) haben sogenannte nationale Vertrauenslisten eine konstitutive Wirkung. Mit anderen Worten, ein Vertrauensdienst und die von ihm erbrachten Vertrauensdienstleistungen werden nur dann qualifiziert und überall in der EU als qualifiziert betrachtet, wenn sie in den sogenannten "Trusted Lists" erscheinen. Folglich profitieren die Nutzer (Bürger, Unternehmen oder öffentliche Verwaltungen) nur dann von der Rechtswirkung eines bestimmten qualifizierten Vertrauensdienstes, wenn dieser in den Vertrauenslisten als qualifiziert aufgeführt ist. Swisscom ist mit seiner Tochtergesellschaft in Österreich "Swisscom IT Services Finance S.E.", Wien in dieser Vertrauensliste aufgenommen worden mit qualifizierten Zertifikaten und Siegeln:

https://webgate.ec.europa.eu/tl-browser/#/tl/AT

Swisscom IT Services Finance S.E. hat Swisscom (Schweiz) AG mit dem Betrieb des Vertrauensdienstes beauftragt und auch die Registrierungsstellentätigkeit an Swisscom (Schweiz) AG delegiert. Swisscom(Schweiz) AG bietet somit den Dienst am Markt an und nimmt auch vertragliche Dokumente im Auftrag der Swisscom IT Services Finance S.E. entgegen.

(62) Kann Swisscom die Rechtssicherheit für ein mit seiner Signatur unterzeichneten Vertrag garantieren?

Swisscom kann grundsätzlich nur bestätigen, dass es nach der eIDAS Verordnung der EU und nach dem ZertES Gesetz der Schweiz in beiden Rechtssystemen qualifizierte Signaturen ausstellen kann. Hierbei werden die qualifizierten Schweizer Signaturen nur in der Schweiz qualifiziert anerkannt und die eIDAS qualifizierten Signaturen in der EU.

Ob die qualifizierte Signatur für einen beliebigen Vertrag zulässig ist, muss in jedem Falle von einem Juristen geprüft werden. Swisscom darf hierzu keinerlei Rechtsauskunft geben. Das hängt nicht nur mit der Signatur zusammen, sondern auch aufgrund ggfs. anderer Punkte, die in Verträgen vereinbart werden können. Beispielsweise kann die Forderung einer "Rücksendung per Einschreiben" dazu führen, dass eine elektronische Signatur gar nicht geleistet werden kann, da ein postalischer Papierweg vorgeschrieben ist.

(63) Hat die qualifizierte Signatur eine stärkere Beweiskraft?

Grundsätzlich gilt in beiden Rechtssystemen EU und Schweiz die Beweisumkehr (bzw. in Deutschland auch Anscheinsbeweis gegenüber dem Augenscheinsbeweis) in Bezug auf qualifizierte Signaturen. D.h. eine Gegenseite muss beweisen, dass die qualifizierte Signatur nicht ordnungsgemäss erfolgt ist, falls diese angefochten wird. Und natürlich kann Swisscom anhand der von KPMG testierten Überprüfungen nachweisen, dass die qualifizierte Signatur ordnungsgemäss erfolgt.

(64) Kann die Gültigkeit einer Signatur auch nach 10 Jahren noch bewiesen werden?

Die Aufbewahrungsfristen der Identitätsfeststellung und des Tätigkeitjournals und damit auch die Beweisfristen betragen in der Schweiz 11 Jahre und in der EU 35 Jahre. Swisscom verwendet grundsätzlich den Langzeitvalidierungsstandard von ETSI (LTV).

Long Term Validation bedeutet eine Signatur so zu validieren, dass sie für lange Zeit valide bleibt. Die LTV Validierung lässt eine Validierung aber nur so lange zu, wie das Wurzelzertifikat für den Zeitstempel nicht abgelaufen ist. Es empfiehlt sich daher bei Langzeitbeweiserhaltung die Dokumente vor Ablauf nochmals mit einem Zeitstempel zu versehen, damit die Integrität und Aussagekraft des Signaturbeweises weiterhin gegeben ist.

Grundsätzlich sollten PDF Dokumente auch in sicheren Archiven verwaltet werden. Es kann eine Situation in 5, 10 oder 20 Jahren kommen, dass die Signaturalgorithmen "geknackt" werden, d.h. es könnte damit die Unversehrtheit oder Authentizität nicht mehr gewährleistet sein. Gute Archivsysteme sehen daher regelmässige Resignatur z.B. mit einem Zeitstempel vor, der immer den neuesten Algorithmus nutzt und damit die Integrität des Dokumentes sicherstellt.

Im WWW findet man hierzu verschiedene optimierte Verfahren, z.B. "Archisig". Das deutsche BSI hat auch eine technische Richtlinie „Beweiswerterhaltung kryptographisch signierter Dokumente“ herausgebracht. Sie ist die Spezifikation sicherheitstechnischer Anforderungen für den langfristigen Beweiswerterhalt von kryptographisch signierten elektronischen Dokumenten und Daten nebst zugehörigen elektronischen Verwaltungsdaten (Metadaten).

Eine für diese Zwecke definierte Middleware (TR-ESOR-Middleware) im Sinn dieser Richtlinie umfasst alle diejenigen Module und Schnittstellen, die zur Sicherung und zum Erhalt der Authentizität und zum Nachweis der Integrität der aufbewahrten Dokumente und Daten eingesetzt werden.

(65) Wie werden Änderungen der gesetzlichen Grundlagen gehandhabt?

Aus der Erfahrung heraus gibt es Übergangsfristen, die von 3 Monaten bis zu 2 Jahre dauern können.

(66) Lässt sich eine Vervielfältigung von signierten Originaldokumenten verhindern?

Nein.

(67) Gibt es im Web Berichte von Kunden von Swisscom, die die digitale Signatur verwenden?

Ja, z.B.:

https://www.seantis.ch/blog/digitale-signatur-onegov-cloud/

https://www.bcge.ch/pdf/conditions-self-en.pdf

https://www.inside-it.ch/articles/49769

(68) Wie wirken sich Zeitstempel auf unterschiedliche Zeitzonen aus?

Grundsätzlich wird bei einem Zeitstempel die Zone mitgespeichert (das Offset). Insofern werden alle lokale Programme die tatsächliche Ortszeit anzeigen.

(69) Adobe meldet den Fehler, dass die Signatur ungültig ist, da sie nicht validiert werden konnte.

"Unterschrift ist gültig jedoch konnte die Sperrung der Identität des Unterzeichners nicht überprüft werden" lautet die Aussage von Adobe, wenn kein LTV Format verwendet wurde. Hintergrund ist, dass dann Adobe bei einem 10 Minuten Zertifikat noch versucht die Gültigkeit zu prüfen. Wurde kein Langzeitvalidierungsformat verwendet, welches die Gültigkeitsinformationen zum Zeitpunkt der Signatur abspeichert, kann auf diese nach einiger Zeit nicht mehr zugegriffen werden. Daher sind Signaturen mit Kurzzeitzertifikaten (aber auch langzeitbeweisbare Signaturen) immer im LTV Format abzuspeichern.

(70) Welche Daten werden im Zertifikat als Distinguished Name (DN) der Personenzertifikate veröffentlicht?

Der Distinguished Name enthält entweder den Vornamen, Nachnamen und das Geburts-/Registrierungs- oder Heimatland der Person oder ein Pseudonym mit einer Seriennummer, die sich durch die Registrierungsstelle eindeutig auf eine Person zurückführen lässt. Organisationsnamen werden nur in Sonderfällen zugelassen.

(71) Welche Dateiformate können signiert werden?

Grundsätzlich liefert Swisscom einen signierten Hash und unterstützt damit PADES (PDF) Formate und bei Organisationszertifikaten auch XADES (XML) Formate. Worddateien werden nicht signiert, sind aber auch gesetzlich hierfür nicht vorgesehen.

10 Datenschutz

(72) Datenschutz in der Schweiz und die DSGVO?

Die Schweiz ist nicht in der EU und hat somit national nicht die Gesetzgebung der EU, die sogenannte Datenschutz-Grundverordnung (DSGVO) eingeführt. Grundsätzlich ist die DSGVO auch dann anwendbar, wenn die Unternehmen ihren Sitz in der Schweiz haben und Dienstleistungen in der EU anbieten.

Somit gelten für Swisscom die gleichen Pflichten im Umgang mit den Daten wie für alle anderen Organisationen, die die DSGVO einhalten müssen:

- informieren und die Einwilligung der Person einholen, deren Daten verarbeitet werden
- "Privacy by design" und "Privacy by default" garantieren
- einen Vertreter für Datenschutzfragen benennen
- ein Verzeichnis der Verarbeitungstätigkeiten erstellen
- Verletzungen des Datenschutzes an die Aufsichtsbehörde melden
- eine Datenschutz-Folgenabschätzung durchführen

Alle Applikationen, die den Datenschutz betreffen und zur Datenverarbeitung eingesetzt werden, z.B. auch die RA-App müssen DSGVO konform sein. Swisscom gibt hierfür auf seinen Seiten:
Schweiz: www.swisscom.com/signing-service

Österreich: www.swisscom.at

Entsprechende Datenschutzerklärungen gemäss DSGVO ab.

Schweiz galt immer schon und gilt gemäss Art. 45 DSGVO (Datenübermittlung auf der Grundlage eines Angemessenheitsbeschluss) als sicheres Drittland, d.h. die üblichen Genehmigungen wie bei anderen Drittländern (z.B. USA) sind hier nicht notwendig. Die Schweiz verfügt dank ihres Datenschutzgesetzes und der laufenden Anpassung an die DSGVO über ein "angemessenes Schutzniveau für die Übermittlung von personenbezogenen Daten" nach EU-Kriterien, d.h. ist faktisch bei der Datenübertragung so wie ein EU Land zu behandeln:

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

(73) Einhaltung des Datenschutzes des All-in Signing Services

Swisscom muss im Rahmen seiner fortlaufenden Auditierungen sowohl gegenüber der Anerkennungsstelle in der Schweiz als auch gegenüber der Konformitätsbewertungsstelle in Österreich, dass alle für die Ausstellung von digitalen Signaturen notwendigen strengen Datenschutzauflagen eingehalten werden. D.h. über einer Selbstdeklaration hinaus sind Vertrauensdienstanbieter und Zertifizierungsdienste durch die Gesetzgebung und den angewandten internationalen Normen, wie z.B. ETSI 319 401, verpflichtet einen angemessenen Datenschutz aller persönlichen Daten nachzuweisen und auditieren zu lassen.

(74) Datenschutz und RA-App/RA-Service

Die nachzuweisenden und zu auditierenden Datenschutzanforderungen gelten auch für die Registrierungsstellentätigkeit – einer Aufgabe eines Vertrauensdienstanbieters und Anbieters von Zertifizierungsdiensten. Damit ist auch der Datenschutz auf der RA-App als Teil des Registrierungsprozesses gewährleistet. Die RA-App selber speichert keine persönlichen Daten permanent. Es können auch keine Daten exportiert werden. Sobald die Identifikation abgeschlossen wurde, werden die Daten vom RA-Agenten signiert übermittelt als sogenannte Evidenz. Diese Evidenzen werden bei Swisscom im RA-Service unter strengen Sicherheitsauflagen (z.B. 4-Augen Zugang) aufbewahrt. Nur wenige Personen haben Zugang zu diesen Daten und dürfen diese nur aufgrund eines richterlichen Beschlusses weitergeben oder in Bezug auf die Qualität der Identifikation prüfen. Swisscom haftet nach dem Gesetz für die ordnungsgemässe Durchführung der Signatur und damit auch der Identifikation unbegrenzt.

RA Master Agenten haben einen Webzugang auf ein Portal, in welchem sie alle von den RA-Agenten identifizierten Personen mit Namen, Vornamen, Ablaufdatum des ID Dokumentes und Mobilfunknummer einsehen können. Die Ausweisdokumente und Fotos (sogenannte "Evidenzen") sind nicht zugreifbar oder exportierbar.

(75) Wozu eine Auftragsdatenverarbeitung?

Swisscom ist gesetzlich verpflichtet, für die Signatur Personendaten aufzunehmen. Sie ist damit für diese Daten verantwortlich. Somit kann Swisscom auch nicht die Rolle eines Auftragsverarbeiters spielen, auch wenn es für die Signatur z.B. Mitarbeiterdaten eines Kundenunternehmens erhält. Ähnlich wie Telekom- oder Postdienstleister hat hier Swisscom einen gesetzlichen Auftrag. Swisscom hat wiederum mit den Nutzungsbestimmungen ein gesetzliches Vertragsverhältnis mit den Signierenden. Hierin akzeptiert der Signierende auch die Datenverwendung.

Mit der RA-App verlagert Swisscom die Aufnahme von Identitätsdaten an einen externen Dienstleister, der in den Verträgen "RA-Agentur" genannt wird. Hierfür sieht die Datenschutzgrundverordnung die Auftragsverarbeitung vor. Die RA-Agentur muss die Vorgaben der Auftragsdatenverarbeitung daher einhalten.

Auch in rein Schweizer Projekten wird die Einhaltung der DSGVO Auftragsdatenverarbeitung eingefordert. Das hat zwei Gründe:

- Einerseits kann selten garantiert werden, dass in der Schweiz identifizierte Personen nicht EU Bürger sind, die dem Marktprinzip der DSGVO unterliegen,
- Andererseits kann die RA-App nicht so eingesetzt werden, dass nur Personen für die Schweiz identifiziert werden, d.h. es findet immer eine Auftragsdatenverarbeitung auch für Swisscom IT Services Finance S.E. in Wien statt.

(76) Welche Pflichten übernehmen RA Agenturen im Rahmen ihrer Tätigkeit?

RA Agenturen sind tätig im Auftrag der Registrierungsstelle von Swisscom. Neben den Pflichten zur gewissenhaften Durchführung der Registrierungsstellentätigkeit steht auch der Datenschutz im Vordergrund. Hier gelten die Datenschutzgrundsätze aus Art. 28 DSGVO, die sich in genauer Form in den technisch-organisatorischen Massnahmen (TOM) im RA-Agentur Vertrag wiederfinden. Sie basieren insbesondere auf 2 Abschnitte des Art. 28, die den Einsatz der App auf dem Mobilgerät reflektieren:

- Die Massnahme muss "die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen" und
- "ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung" einschliessen.
- Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

D.h. neben dem Einsatz von gewissenhaften und geschulten Mitarbeitern muss insbesondere der Schutz der App auf dem Mobilgerät und auch der Schutz des Zugangs gewährleistet sein. Werden die Geräte geeignet gegen Viren geschützt? Wird der Download von Programmen aus fremden App-Stores, die nicht ausreichenden Schutz bieten untersagt? Halten die Mitarbeiter ihre PINs, Passwörter geheim? Werden Geräte nicht gerootet?

(77) Identifikationsprozess mit eigenen Daten benötigen keine Auftragsdatenverarbeitung?

Es gibt Projekte, in denen Swisscom auf gesetzlich anerkannte Identifikationsverfahren bei Dritten aufsetzt und diese auch auditieren lässt. Typisches Beispiel ist hier eine Bank, die im Rahmen ihres KYC Prozesses eine Präsenzidentifikation einer Person durchführt. In diesem Falle erhält Swisscom eine Kopie dieser Daten für ihre eigene Geschäftszwecke (Signatur). Eine Auftragsdatenverarbeitung ist hier nicht notwendig, da zwei verantwortliche Parteien für die Daten vorhanden sind. Umgekehrt wird hierbei auch nicht das Joint Controllership Prinzip der DSGVO herangezogen, da die Aufnahme nicht einem gleichen Geschäftszweck dient und beide im Sinne des gemeinsamen Geschäftszwecks verantwortlich handeln. Die Bank handelt für ihren Geschäftszweck, z.B. Kontoeröffnung und Swisscom verfolgt seinen Geschäftszweck, die Ausstellung von Signaturen. Dennoch beinhalten unsere Verträge zur "Delegation der Registrierungsstellentätigkeit" in diesem Fall auch ein Minimum an Regelungen, wie in Bezug auf Datenschutz und DSGVO vorgegangen wird.

(78) Wie hebt Swisscom die privaten Schlüssel zu den Signaturzertifikaten auf?

Bei einer Fernsignatur verwaltet Swisscom treuhänderisch die Schlüssel zu den Signaturzertifikaten. Bei einer Personensignatur werden die Signaturzertifikate nur für die Signatur erzeugt und verlieren nach ca. 10 Minuten ihre Gültigkeit. Unternehmenszertifikate für Siegel haben Gültigkeiten von bis zu 3 Jahren. Der private Schlüssel muss dabei laut Gesetz auf einer (qualifizierten) Signaturerstellungseinheit gespeichert werden. Der Speicher hierfür ist ein Gerät, welches hauptsächlich nur für die Schlüsselspeicherung konzipiert ist, das HSM (Hardware Security Modul). Es unterliegt einer strengen Regulierung, Auditierung, in Bezug auf Fähigkeiten und Zugang zu diesem Gerät. Für Signaturen in der EU und in der Schweiz gelten besonders hohe Fähigkeiten, die nur von wenigen HSM Herstellern weltweit zur Verfügung gestellt werden.

11 Inbetriebnahme

(79) Wie läuft die Inbetriebnahme bei einer Personensignatur ab?

Voraussetzung für die Inbetriebnahme ist eine vom Kunden unterzeichnete und von der globalen Registrierungsstelle geprüften "Konfigurations- und Annahmeerklärung". In dieser werden die Pflichten des Betreibers einer Signaturapplikation festgehalten (z.B. die Möglichkeit der vollständigen Anzeige des zu unterzeichnenden Dokuments, Absicherung des Zugangs zum Service), aber auch die Ausprägung des Service.

Weitere Voraussetzung ist ein Zugangszertifikat, welches die Kommunikation der Signaturapplikation zum Signaturservice absichert.

Nach der Prüfung des Dokumentes erhält unser Setup Service den Auftrag zur Aufschaltung des Service mit dem zugesendeten Zugangszertifikat und der gewählten Ausprägung in der Konfigurations- und Annahmeerklärung. Bei qualifizierter Signatur wird der Service zunächst immer nur auf dem Niveau "fortgeschritten" freigeschaltet. Anschliessend wird der in der Konfigurations- und Annahmeerklärung genannte Ansprechpartner um eine Beispielsignatur mit der fortgeschrittenen Signatur gebeten. Ist diese einwandfrei, wird der Service umgeschaltet auf das Niveau "qualifiziert", sofern dieses verlangt wurde. Hierüber wird der Kunde ebenfalls benachrichtigt. Er hat nun 10 Tage Zeit etwaige Unregelmässigkeiten direkt an das Setup Team zurückzumelden. Sollten diese in dieser Zeit nicht aufgetreten sein, ist der Anschluss an der Service abgenommen. Weitere Incidents können dann über den 1st Level Support an Swisscom gemeldet werden im Falle eines Direktvertrages mit Swisscom, andernfalls an den Reselling Partner.

(80) Welche Voraussetzungen werden an das Zugangszertifikat gestellt?

Das Zugangszertifikat kann ein selbst signiertes Zertifikat sein. Beispielweise mit openssl Software.

Anforderungen an den Distinguished Name:

- CN=<URL des Teilnehmersystems, welches die Kommunikation mit AIS durchführt oder andere eindeutige Identifikation des Teilnehmersystems>
- O=<Name der Organisation>
- Email=<E-Mail Adresse für Informationen am Ende des Gültigkeitszeitraumes>
- C=<Land der Organisation>

Folgende weitere Anforderungen sind bei der Erstellung des Zertifikates zu berücksichtigen:

- Maximale Laufzeit 3 Jahre
- Hashalgorithmus minimum SHA-256
- Key length minimum 2048 bit

Für Zugangszertifikate im Rahmen der geregelten (ZertES) oder qualifizierten (eIDAS) Siegelerstellung gelten noch besondere Bedingungen: Der private Schlüssel des Zugangszertifikates muss in einer gemeinsamen Zeremonie eines Registrierungsstellenvertreters von Swisscom auf einem kryptographischen Modul erstellt werden. Dieses Modul muss den Anforderungen an FIPS 140-2 level 2 entsprechen, z.B. Yubikey oder Microsoft Key Vault.

(81) Wie läuft die Inbetriebnahme eines Siegels ab?

Im Falle eines Siegels benötigt es neben der Konfigurations- und Annahmeerklärung durch den Betreiber der Signaturplattform noch einen Zertifikatsantrag für das Siegelzertifikat, ein Organisationszertifikat. Im Gegensatz zum Zertifikat für die Personensignatur wird das Siegelzertifikat für drei Jahre ausgestellt. Der Zertifikatsantrag muss unterzeichnet werden von berechtigten Personen der Organisation. Die Berechtigung kann sich aus dem Register ergeben (z.B. Prokura) oder auch eine eingeschränkte Handlungsvollmacht sein, die Prokurist z.B. für die Operatoren im Rechenzentrum ausgestellt hat. Hierbei müsste Swisscom dann einen Nachweis dieser Vollmacht erhalten. Diese Personen werden vorab auch noch durch einen Vertreter der Registrierungsstelle von Swisscom persönlich mit RA-App identifiziert. Das kann z.B. auch ein RA-Agent sein, der die persönliche Identifikation vorgenommen hat. Dadurch kann die Person den Antrag mittels elektronischer Unterschrift unterzeichnen. Der Antrag wird hierzu unsigniert an Swisscom zugesendet und Swisscom lädt die Personen zur elektronischen Signatur ein. Jetzt unterscheiden sich die weiteren Schritte je nach Art des Siegels:

Fortgeschrittene Signatur: Der Antragsteller sendet Swisscom ein SSL Zertifikat zu, welches er als Zugangszertifikat für die Schnittstelle zum Siegel verwenden will.

Qualifizierte/Geregelte Signatur: Der Antragsteller vereinbart mit Swisscom einen Termin für eine gemeinsame Erstellung eines privaten Schlüssels. Dieser muss auf einem kryptographischen Device der Qualifizierung FIPS 140-2 level 2 erstellt werden (z.B. Yubikey, Key Vault HSM Microsoft, etc.) Basierend auf diesen Schlüssel wird dann ein Zugangszertifikat erstellt. D.h. für den Signaturvorgang muss der Zugang mittels diesem Zertifikat freigegeben werden.