Als führender Vertrauensdiensteanbieter in Europa ermöglichen wir die innovativsten, digitalen Geschäftsmodelle.

Leistungsbeschreibung
Smart Registration & Signing Service

Swisscom Trust Services

Swisscom Trust Services AG

Konradstrasse 12
8005 Zürich

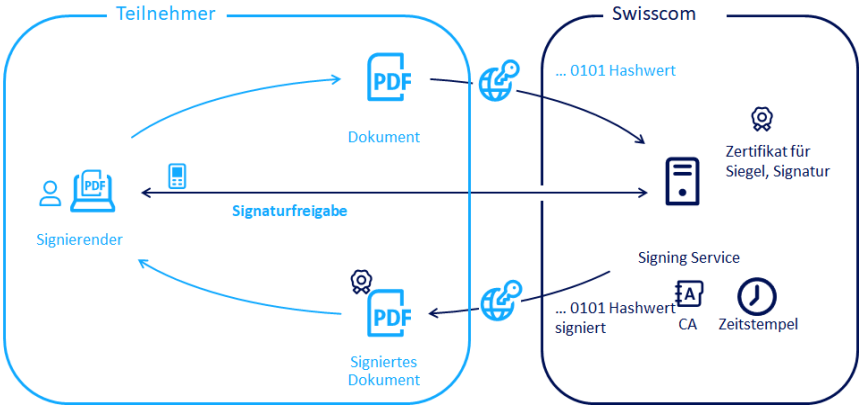
Schweiz

https://trustservices.swisscom.com
E-Mail: sts.salessupport@swisscom.com

1 Inhalt

2 Übersicht zum Service

Der Smart Registration & Signing Service ist eine serverbasierte modular aufgebaute Fernsignaturdienstleistung vertrieben durch Swisscom Trust Services AG und erbracht durch den Zertifizierungsdienst der Swisscom (Schweiz) AG, dem Vertrauensdienst der Swisscom IT Services Finance S.E. (Wien) (nachfolgend «Swisscom ITSF» genannt) und weiteren angeschlossenen Partnern oder Trust Service Providern. Die Signing Service für die Schweiz und EU werden in Rechenzentren in der Schweiz erbracht. Swisscom Trust Services AG vertreibt den Signing Service in eigenen Namen oder räumt Dritten wiederum das Recht ein, den Signing Service in eigenem Namen zu vertreiben.
Die Fernsignaturdienstleistung wird Teilnehmern zur Verfügung gestellt, die eine Teilnehmerapplikation betreiben. Signierende können damit digitale Dateien elektronisch signieren und die Integrität und die Authentizität einer Datei sichern. Swisscom (Schweiz) AG als Zertifizierungsdienstanbieter in der Schweiz oder die Swisscom IT Services Finance S.E. als qualifizierter Trust Service Provider der EU unter eIDAS erzeugt und verwaltet für den Signierenden oder Siegelersteller treuhänderisch das Signaturzertifikat und stellt dieses für die Fernsignaturdienstleistung über einen verschlüsselten Kanal zur Verfügung. Somit benötigt der Signierende für diesen Dienst ausser einer vom Teilnehmer betriebene Teilnehmerapplikation zum Versand des zu signierenden und Empfang des signierten Dokumentes keine weiteren Betriebsmittel, wie z.B. Token oder Signaturkarte.
Die Teilnehmerapplikation bereitet ein Dokument so auf, dass zum Signieren nur der Hash-Wert (Prüfsumme fester Länge ohne Rückschluss auf den Inhalt) an den Signing Service übermittelt wird. Die effektiv lesbaren Dateien und die darin enthaltenen Informationen verlassen die Systemumgebung des Teilnehmers nicht und sind damit für die Swisscom Zertifizierungs- und Vertrauensdienste nicht ersichtlich. Der signierte Hash wird von der Teilnehmerapplikation wieder in das Dokument eingebaut und erzeugt damit ein signiertes Dokument. Vor der Auslösung der Signatur muss der Teilnehmer sich in der Teilnehmerapplikation authentifizieren und die Signatur freigeben.



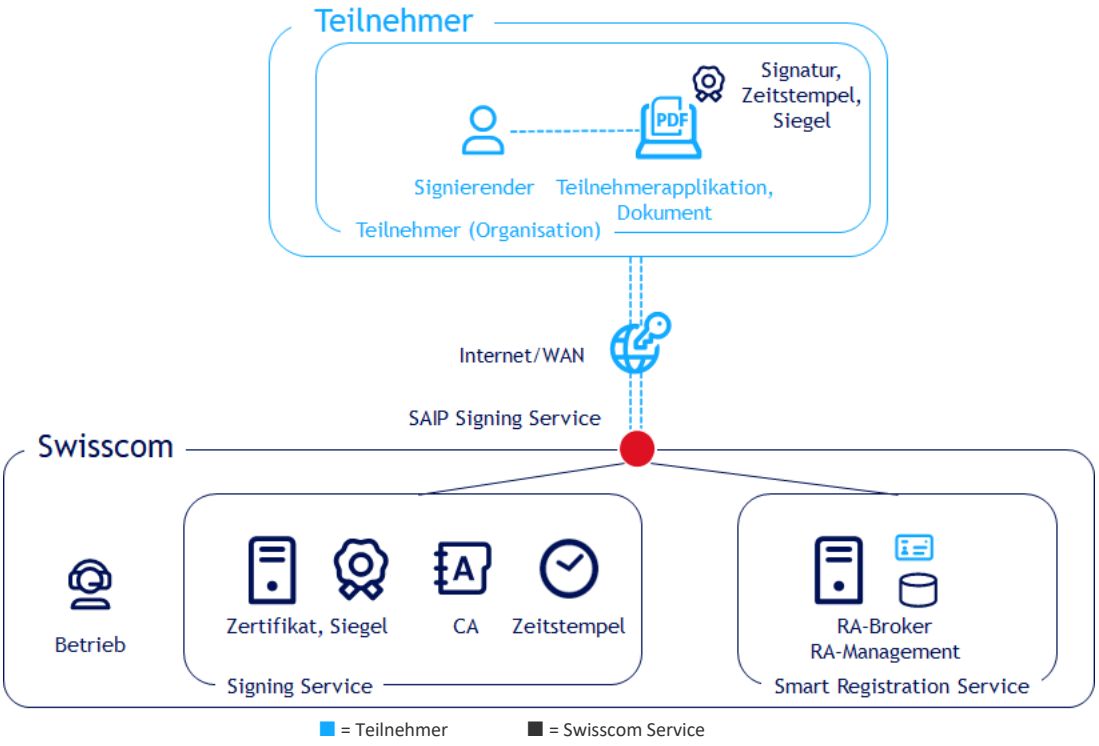
Des Weiteren bietet der Service eine einmalige, zeitlich begrenzte Registrierung und die fortwährende Nutzung eines Signaturfreigabemittels (z.B. Fingerprint App) für die Personensignatur ("Repetitive Signing"). Es wird aber auch eine Einmalidentifikation- und Signatur ("One-shot Signing") angeboten. Für die Nutzung von Identifikations- und Signaturfreigabemethode stehen jeweils Stores (Marktplätze) zur Verfügung, in denen Partner Ihre Methoden für Teilnehmerapplikationen anbieten, für die aber auch die Swisscom Zertifizierungs- und Vertrauensdienste eigene Methoden bereitstellen. Für die Bereitstellung von Siegeln und Zeitstempel kann eine Dauerfreigabe eingerichtet werden. Die Orchestrierung der Registrierung und Signaturfreigabe mit den in den Stores erhältlichen Registrierungs- und Freigabemethoden erfolgt durch den Multiple Authentication Broker. Als Ergebnis der Brokerkommunikation erhält die Signaturapplikation ein Token mit dem dann die Signaturapplikation die Hashsignatur durchführen kann. Der Broker und die verfügbaren Methoden sind in der " Leistungsbeschreibung Registrierungs- und Signaturfreigabemethoden" beschrieben.
Allgemein bietet der Signing Service je nach konkreter Vertragsgestaltung fortgeschrittene und qualifizierte elektronische Signaturen für natürliche Personen, fortgeschrittene und geregelte oder qualifizierte elektronische Siegel für Organisationen sowie Zeitstempel an.
Qualifizierte elektronische Signaturen haben die höchste Rechtswirkung und sind in zahlreichen Fällen der eigenhändigen Unterschrift gleichgestellt. Damit können grundsätzlich auch Geschäftserfordernisse erfüllt werden, die vom Gesetz her eine eigenhändige Unterschrift erfordern (vgl. hierzu Ziffer 8.2).
Swisscom (Schweiz) AG ist in der Schweiz gemäss ZertES anerkannte Anbieterin von Signatur- und Zertifizierungsdiensten, Swisscom ITSF ist für die Ausstellung fortgeschrittener und qualifizierter Zertifikate für elektronische Signaturen und elektronischer Siegel anerkannte qualifizierte Vertrauensdiensteanbieterin gemäss eIDAS-Verordnung und österreichischem Signatur- und Vertrauensdienstegesetz (SVG). Die akkreditierten Anerkennungsstellen prüfen regelmässig, ob die anwendbaren rechtlichen und regulatorischen Anforderungen auch erfüllt werden.

Diese Leistungsbeschreibung beschreibt den Service für elektronische Signaturen für natürliche Personen wohnhaft in der EU, der Schweiz und EWR Staaten, bzw. Siegel und Zeitstempel.

3 Definitionen

3.1 Service Access Interface Point (SAIP)

Der Service Access Interface Point (SAIP) ist der vertraglich vereinbarte, geografische und/oder logische Punkt, an dem ein Service dem Leistungsbezüger (Teilnehmer) bereitgestellt, überwacht und die erbrachten Service Level ausgewiesen werden.
Folgende rein schematische Darstellung dient der Veranschaulichung der Leistungen und Leistungs-Komponenten von Smart Registration & Signing Service:



Der Übergabepunkt der Leistung ist hierbei für die Signaturen der Anschluss am Internet der Swisscom Zertifizierungs- und Vertrauensdienste. Die Verfügbarkeit des Services ist dann gegeben, wenn Anfragen durch den Service entgegengenommen werden und entsprechend der Schnittstellenbeschreibung zum SAIP korrekt beantwortet werden. Die korrekte Antwort kann auch in einer dokumentierten oder für den Teilnehmer aussagekräftigen Fehlermeldung bestehen.
Die Schnittstellenbeschreibung befindet sich unter https://trustservices.swisscom.com/downloads unter dem Link „Reference Guide“:
https://documents.swisscom.com/product/filestore/lib/e2007490-6fd4-4012-801d-b104801a9abc/reference_guide_smartregistration_signing-en.pdf?idxme=pex-search
Sowie dem Guide in der Partner Area:
trustservices.swisscom.com/hubfs/Website Files/Documents/Developer Documentation/MAB-IntegrationGuide-en.pdf
SMS-Informationen werden, sofern nicht innerhalb des Swisscom-Netzwerks erbracht, an der Schnittstelle zum Roaming Partner bereitgestellt. Ein Leistungsversprechen für das Funktionieren des Internets oder des Netzwerkbetriebs des Roaming Partners ist ausgeschlossen.

3.2 Servicespezifische Definitionen

Begriff	Beschreibung
2-Faktor Signaturfreigabe	Qualifizierte elektronische Signaturen, die über Fernsignaturen angeboten werden oder qualifizierte/geregelte Siegel müssen mit einem Signaturfreigabemethode freigegeben werden, bei dem der Signierende 2 Faktoren anwendet. Diese 2 Faktoren müssen aus den drei Bereichen Besitz, Wissen und Sein (Biometrie) kommen. So z.B. der Besitz einer Mobilnummer oder einer App auf dem Smartphone kombiniert mit dem Wissen um ein Passwort oder einer PIN. Oder alternativ kann auch ein biometrisches Merkmal verwendet werden, wie z.B. ein Fingerabdruck.
Access Token	Das Access Token (oder Zugriffstoken) gibt einem Benutzer den Zugriff auf eine Ressource. Das Token identifiziert ihn gegenüber der Ressource. Im Signaturkontext wird zuvor die Identifikation und Signaturfreigabe sichergestellt. Das daraufhin ausgestellte Token ermöglicht den Nutzer eine Signaturanfrage auszustellen und eine Signatur zu erhalten. Im OAuth 2.0 Standard sind sie definiert und können überdies auch noch verschiedene Eigenschaften haben, z.B. eine begrenzte Lebenszeit.
Audit	Konformitätsbewertungsstellen prüfen im Rahmen eines Audits die Konformität des Zertifizierungs- oder Vertrauensdienstes im Zusammenhang mit dem anwendbaren Recht und den anwendbaren Normen.
Anerkennungsstelle	Nach ZertES sind die Anerkennungsstellen für die Anerkennung von Zertifizierungsdiensten zuständig. In der Schweiz ist derzeit die KPMG die einzige Anerkennungsstelle. Das Pendant in der eIDAS Verordnung hierzu ist die Aufsichtsstelle.
Aufsichtsstelle	Nach eIDAS-VO ist eine Aufsichtsstelle damit beauftragt, die Qualifizierung der entsprechenden Vertrauensdienste sicherzustellen und damit die Sicherstellung eines vergleichbaren Sicherheitsniveaus. Sie bedient sich dabei dem Auditbericht der Konformitätsbewertungsstellen. Im Schweizer Signaturgesetz ZertES findet sich das Pendant der Anerkennungsstelle.
Authorization Code	Im OAuth2.0 Standardprotokoll ist der Authorization Code ein temporärer Code den ein Client System nutzen kann, um ein Access Token zu erhalten. Das verhindert z.B. einen sichtbaren Austausch des Access Tokens über eine Browserschnittstelle, so dass ein Angreifer verhindert ist, den Access Code abzufangen.
CEN/TS 419 241	CEN ist ein europäisches Komitee für Normung, welches mit dem Standard 419 241 einen Standard für Fernsignaturen herausbrachte. In diesem Standard wird unter anderem der Zugriff auf eine Signatur und damit auch die Signaturfreigabe normiert. Er ist im schweizerischen Signaturrecht verankert und wird auch von verschiedenen Aufsichtsstellen in Europa für die Zulassung von Fernsignaturanbietern eingefordert.
Claimed ID	Die Claimed ID ist das Zugangskonto zum Signing Service der Swisscom Trust Services. Es besteht aus einem eindeutigen Kennzeichen für den Teilnehmer (z.B. die URL seiner Homepage) und dem Zusatz, welche Zertifikate bei der Signatur verwendet werden.
CMS	Cryptographic Message Syntax – Eine im RFC5652 definierte Syntax für die digitale Signatur und kryptographische Mitteilungen
CP/CPS (Zertifikatsrichtlinien)	Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten der Klasse "Diamant“ (qualifiziert) und „Saphir“ (fortgeschritten). Zertifikatsrichtlinien und Zertifikatspraxis sind Dokumente einer Zertifizierungsstelle, die die Richtlinien und Praxis zur Ausstellung von Zertifikaten beschreiben. Diese befinden sich im Repository unter https://trustservices.swisscom.com/repository

Begriff	Beschreibung
Distinguished Name	Ein Zertifikat enthält auch ein Verzeichnis mit Informationen zum Zertifikatsinhaber, z.B. zum Signierenden. Das Verzeichnisobjekt, welches den Zertifikatsinhaber charakterisiert, wird „Distinguished Name“ genannt. Es enthält wiederum Parameter, wie z.B. den „Common Name“ (gebräuchlichen Namen, den „surname“ oder „last name“ (Vor- bzw. Nachnamen), „country“ (Ausstellungsland der Signatur oder des Ausweises oder der Registrierungsstelle), „serial number“ (eindeutige Seriennummer) aber auch „organization“ (Organisation, zu der der Zertifikatsinhaber gehört) oder „organizational unit“ (Unterorganisation).
DSG	Bundesgesetz über den Datenschutz der Schweiz. Die Fassung vom 1. September 2023 ist in grossen Teilen angeglichen an die Datenschutzgesetzgebung der EU (DSGVO).
DSGVO	Datenschutzgrundverordnung der EU. EU-Regulierung zum Datenschutz.
Dokument	Der Begriff Dokument wird, zur besseren Verständlichkeit, synonym für den Begriff Daten benutzt. Es können sowohl Dokumente als auch Daten signiert werden.
eIDAS-VO	Verordnung Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG); regelt insbesondere auch die elektronische Signatur. Auf nationaler Ebene gibt es typischerweise sogenannte “Umsetzungsgesetze”, die gegebenenfalls noch Aspekte national regeln, die in der Verordnung nicht geregelt wurden. In Österreich ist das das SVG (Signatur- und Vertrauensdienstegesetz), welches z.B. den Aspekt der Archivierungsdauer für Daten regelt.
HSM	Sofern qualifizierte (EU) oder geregelte (CH) Siegel ausgestellt werden, wird über einen mit TLS-Zugangszertifikat geschützte Schnittstelle die Freigabe der Siegel sichergestellt. Hierfür muss der Verantwortliche des Siegelerstellers den privaten Schlüssel des Zugangszertifikates entsprechend aufbewahren und verwalten, damit er hierüber die Freigabe steuern kann. Die Lösung hierfür ist vom Partner in den Einsatzbedingungen für die Siegelerstellung zu beschreiben. Anschliessend wird Swisscom Trust Services diese Lösung prüfen und mit dem Teilnehmer einen Vertrag zur «Freigabelösung Siegel» abschliessen.
Elektronische Signatur	Die elektronische Signatur erlaubt die Anwendung eines technischen Verfahrens zur Überprüfung der Integrität eines Dokuments, einer elektronischen Nachricht oder anderer elektronischer Daten sowie der Identität des Signierenden. Sie bedient sich dabei den technischen Möglichkeiten eines Zertifikates.
Elektronisches Siegel	Das elektronische Siegel basiert in technischer Hinsicht auf den genau gleichen Verfahren wie die elektronische Signatur. Elektronisches Siegel sind Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen. Nach Schweizer Recht sind nur geregelte elektronische Siegel für UID-Einheiten gesetzlich geregelt, nicht hingegen fortgeschrittene elektronische Siegel. In der eIDAS Verordnung sind sowohl qualifizierte als auch fortgeschrittene Siegel gesetzlich geregelt.
ETSI EN 119 432	Protokoll aus 2021 der Standardisierungsorganisation des Europäischen Instituts für Telekommunikationsnormen (ETSI) für den Anschluss einer Signaturapplikation an ein Fernsignatursystem.
Evidenz	Datensammlung, die den Nachweis einer Registrierung und insbesondere auch die Identität eines Signierenden bezeugen kann. Dieser Nachweis kann auch aus einem Verweis auf einen Datensatz (Evidenz) bestehen, die von einer delegierten Registrierungsstelle verwaltet wird.
Freigabelösung Siegel	Von Swisscom Trust Services und dem Ersteller einer Siegel Teilnehmerapplikation unterzeichneter Vertrag zum Einsatz einer Siegellösung inklusive der Verwaltung des privaten Schlüssels des Zugangszertifikates.

Begriff	Beschreibung
Hash	Fingerabdruck bzw. eindeutige Abbildung eines Dokumentes, d.h. eine grosse Zeichenfolge (z.B. das Dokument) wird umgewandelt in eine kleine charakteristische Zeichenfolge, die aber eindeutig nur so aus der grossen Zeichenfolge entstehen kann. Damit können alle Signaturoperationen am Hash erfolgen und müssen nicht am Dokument selbst erfolgen. Aus dem Inhalt des Hashs kann nicht auf den Inhalt des Dokumentes geschlossen werden, d.h. nur umgekehrt kann auf Basis des Dokumentes der Hash ermittelt werden.
HSM	Hardware Sicherheitsmodul (Hardware Security Module) bezeichnet ein Gerät für die effiziente und sichere Ausführung von kryptographischen Operationen. Insbesondere die privaten Schlüssel zu den Zertifikaten werden hier erzeugt und verwaltet und bieten damit bestmöglichen Schutz gegen einen Angriff von aussen.
IdP	Identity Provider: Eine externe Registrierungsstelle, die eine Identität einer Person bestätigt typischerweise durch eine Authentisierung und Abgleich mit einer Identitätsdatenbank. Das Authentisierungsverfahren kann später auch zur Signaturfreigabe genutzt werden. Im Smart Registration Service kommuniziert der IdP mit dem Multiplen Authentication Broker. Der Authentication Broker erfährt nach der Registrierung aus der RA / Evidenz-Datenbank, für welche Signierende welcher IdP zuständig ist. Sofern der IdP sich bei der Authentisierung auf bereits vorhandene Identitätsprüfungen stützen kann, die auditiert für die elektronische Signatur verwendet werden dürfen, erfolgt auch die Registrierung mit einer erstmaligen Authentisierung und Akzeptanz der Nutzungsbestimmungen. Beispiel: eine Bank. Ein IdP kann aber auch nur das Authentisierungsmittel als Signaturfreigabemethode zur Verfügung stellen und dieses koppeln lassen mit den Ergebnissen eines Identitätsprüfers.
Konformitätsbewertungsstelle	Konformitätsbewertungsstellen sind national akkreditiert und befugt, Zertifizierungsdiensteanbieter oder Vertrauensdiensteanbieter zu auditieren und zu zertifizieren. Der Bericht einer Konformitätsbewertungsstelle wird der Aufsichtsstelle vorgelegt.
LTV / Langzeitvalidierung	Wird eine Signatur mit einem Zeitstempel erstellt und der Signatur noch verschiedene Informationen zur Revokation bzw. Gültigkeit des Signaturzertifikats und der übergeordneten ausstellenden Zertifikate und Rootzertifikate mitgegeben, so enthält die Signatur alle Prüfinformationen, die es erlauben diese Signatur auch in Zukunft zu überprüfen, wenn das Signaturzertifikat selbst oder das ausstellende Zertifikat oder das Rootzertifikat seine Gültigkeit verloren hat. Zu den Gültigkeitsinformationen zählen auch die Zertifikate für den Gültigkeitsdienst, den sognannten OCSP-Service (Online Certificate Service Protocol), bei dem online Gültigkeiten von Zertifikaten angefragt werden können. Solcher Signaturen sind langzeitvalidierbar.
Mobile ID	Managed Service für die sichere Benutzer-Authentisierung. Mobile ID kann von verschiedenen Providern, unter anderem Swisscom (Schweiz) AG, bezogen werden.
Mobile ID App	Managed Service App (Applikation), die vom Google Play Store oder Apple Store herunter geladen werden kann zur sicheren Benutzer-Authentisierung. Diese basiert auf Authentisierungsmöglichkeiten des Mobilgerätes wie z.B. Fingerprint oder Face Recognition. Die Mobile ID App wird über eine internationale Mobilnummer initialisiert und funktioniert mit einer laufenden Internetverbindung.
Multiple Authentication Broker (MAB)	Interne Komponente im Smart Registration Service, welche sämtliche Kommunikation nach aussen in Bezug auf Registrierung und Signaturfreigabe sicherstellt und koordiniert welche Gestützt auf die Logik der Registrierungsstelle und ihrer RA Datenbank entscheidet der Multiple Authentication Broker, welche Signaturfreigabemethode, bzw. welcher externer IdP für die Signaturfreigabe angesprochen werden muss. Er stellt die Signaturfreigabedurchführung sicher – ggfs. durch Aufruf einer Registrierung für nicht registrierte Signierende. Nach erfolgter Signaturfreigabe ermöglicht der Broker dem Teilnehmer den Bezug eines Zugangstoken, um die Signatur beim Signing Service anzufragen.

Begriff	Beschreibung
Nutzungsbestimmungen (Subscriber Agreement)	Bestimmungen, die - gesetzlich vorgeschrieben - jeder Nutzer vor Zusammenarbeit mit einem Vertrauens- oder Zertifizierungsdienst akzeptieren muss. Sie müssen nicht unbedingt signiert werden, aber die Akzeptanz muss im Rahmen der Registrierung nachweisbar sichergestellt werden. Die Nutzungsbestimmungen regeln im direkten Verhältnis zwischen Swisscom (Schweiz) AG und dem Signierenden bzw. der Swisscom ITSF und dem Signierenden auf einer Teilnehmerapplikation die Bedingungen für die Nutzung der Signaturzertifikate und Signaturdienstleistung. Diese sind unter https://trustservices.swisscom.com/repository/ abrufbar..
OAuth	OAuth 2.0 steht für Open Authorization und ist ein Standard, mithilfe dessen eine Website oder Anwendung auf Ressourcen zugreifen kann, die von einem anderen Service angeboten werden. Es ist der massgebliche Branchenstandard für die Online-Autorisierung.
Open ID Connect	Ist eine Authentifizierungsschicht, die auf dem OAuth 2.0 Framework basiert und dazu dient, die Identität eines Nutzers mit Hilfe von Authentifizierungsserver zu überprüfen, beispielweise über einen IdP. Der Standard wird von der OpenID Foundation herausgegeben.
OTP	Einmalcode, der für eine einfache Nutzung via SMS an ein Mobilfunkgerät übertragen wird. Damit wird der Faktor „Besitz“ eines Mobilfunkgerätes mit der angegebenen Mobilnummer überprüft.
OU Eintrag	Eintrag der Organisatorischen Einheit (organizational unit), einem Bezeichner im Distinguished Name eines Zertifikates, der die Organisationseinheit unter der führenden Organisations angibt.
PAdES	PAdES (PDF Advanced Electronic Signatures) ist eine Menge von Einschränkungen und Erweiterungen für PDF-Dateien, damit diese für elektronische Signaturen besser nutzbar sind. Sie sind von dem European Telecommunications Standard Institute (ETSI) im Rahmen von ETSI EN 319 412 standardisiert worden. In der EU ist der Standard verbindlich vorgeschrieben für elektronisch signierte Dokumente durch den EU-Durchführungsbeschluss 2015/1506 der EU-Kommission.
Passkeys	Passkeys sind eine Erweiterung des FIDO-Standards für eine 2-Faktor Authentisierung, die typischerweise von Webdiensten auch für die Anmeldung genutzt wird. Es handelt sich dabei um Paare von privaten und öffentlichen Schlüsseln, die auf dem jeweiligen Gerät gespeichert werden und innerhalb einer Android/Apple oder Windows Umgebung auch in der jeweiligen Umgebung auf mehreren Geräten synchronisiert werden. Typischerweise wird zur Aktivierung der Passkeys die Methode zu dem Entsperren des Bildschirms verwendet (z.B. Fingerprint, Gesichtserkennung oder PIN). Alternativ können auch FIDO2 kompatible USB- oder NFC Sticks genutzt werden. Damit ist eine Signaturfreigabe unabhängig von einer Mobilnummer oder sogar unabhängig von einem Smartphone möglich.
Personensignatur	Signaturen durch natürliche Personen im Gegensatz zu Siegeln.
PKCS#1	Kryptographischer Standard der RSA Laboratories für die Verschlüsselung.
PWD	Password (-eingabe), für die Authentisierung am Service oder Signaturfreigabe zu verwendendes Password, welches den Faktor «Wissen» bietet.
RA	Registration Authority - Registrierungsstelle
RA-Agent	Autorisierter Bediener der RA-App
RA-Agentur	Organisation, die die RA-Agenten stellt
RA-App	App (Applikation), die im Store von Android oder iOS heruntergeladen wird. Diese ermöglicht einem ausgebildeten RA-Agenten die Identifikation für fortgeschrittene und qualifizierte Signaturen und überträgt die Daten an den RA-Service der Swisscom Trust Services. Die RA-Agenten arbeiten hier im Auftrag der Registrierungsstelle des Swisscom Zertifizierungs- und Vertrauensdienstes.
RA-Service	Service zur Entgegennahme und Archivierung der Evidenzen, Betrieb in Zusammenhang mit der RA App oder anderen Registrierungsmethoden.
Registrierungsstelle (RA), RA-Stelle	Interne oder (teilweise) externe delegierte Stelle, die die Registrierung übernimmt.

Begriff	Beschreibung
Registrierung	Eine Registrierung besteht immer aus einer Identifizierung, Akzeptanz der Nutzungsbestimmungen und Zuweisung und Überprüfung einer Signaturfreigabemethode.
RFC3161	RFC (Request for Comment) ist ein Internetstandard. Mit RFC 3161 wird das Zeitstempelprotokoll standardisiert und legt dabei genau die Formate der Anfrage an einen Zeitstempeldienst und die Antworten fest. Swisscom Trust Services richtet sich dabei genau an die Formate dieses Protokoll, bettet aber die Anfrage in die eigene Signing Service Schnittstelle ein, auch zu Abrechnungszwecken. D.h. es wird keine sogenannte RFC 3161 URL zur Verfügung gestellt.
RoW	Rest of World – gemeint sind damit die Staaten ausserhalb der Schweiz, die nicht zur EU oder dem EWR zugehörig sind,
Schlüssel	Eine elektronische Signatur stützt sich zunächst auf ein Schlüsselpaar, welches im HSM erzeugt wird. Des Weiteren wird vom Dokument ein Hash gebildet. Dieser Hash wird mit dem privaten Schlüssel verschlüsselt, so dass er später mit dem öffentlichen Schlüssel entschlüsselt werden kann. Die Signaturprüfung erfolgt dann umgekehrt: Es wird wiederum ein Hash vom Dokument gebildet. Mit dem öffentlichen Schlüssel wird der verschlüsselte Hash entschlüsselt und überprüft, ob er mit dem frisch gebildeten Hash des Dokumentes übereinstimmt. Ist das nicht der Fall, wurde das Dokument entweder verändert, oder der öffentliche Schlüssel passt nicht zum privaten Schlüssel, d.h. das Dokument wurde von jemandem anders signiert.
Signaturzertifikat bzw. Siegelzertifikat	Zertifikat, welches auf den Signierenden bzw. den Siegelersteller ausgestellt ist, von den Swisscom Zertifizierungs- und Vertrauensdiensten treuhänderisch verwaltet wird und zur Signatur bzw. Siegelerstellung verwendet wird.
Siegelersteller	Organisation (juristische Person, Verwaltungseinheiten etc.), die eine UID-Einheit ist im Sinne des Artikels 3 Absatz 1 Buchstabe c des schweizerischen Bundesgesetzes vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer (UIDG) oder juristische Person im Sinne der eIDAS-VO, in deren Namen ein digitales Zertifikat von den Swisscom Zertifizierungs- und Vertrauensdiensten ausgestellt wurde, auf Basis dessen sie ein fortgeschrittenes oder qualifiziertes elektronisches Siegel erstellt. Zukünftige Siegelersteller müssen beim entsprechenden Swisscom Zertifizierungs- oder Vertrauensdienst zunächst einen Antrag auf Ausstellen eines digitalen Zertifikats stellen. Bis zur Genehmigung des Antrags durch den betreffenden Swisscom Zertifizierungs- oder Vertrauensdienst sind Siegelersteller Antragsteller (die bei Ablehnung des Antrags keine Siegel erstellen können).
Signaturfreigabemethode	technisch gesehen ein Authentifizierungsmittel oder eine Methode, die während der Registrierung geprüft wurde. Es stellt mittels 1-Faktor (fortgeschritten) oder 2 unterschiedliche Faktoren aus zwei von drei Typen (Besitz, Wissen, Biometrie) (qualifiziert) die während der Registrierung geprüfte Identität sicher. Es wird dazu verwendet, dass der Signierende den alleinigen Zugriff auf den Schlüssel des Signaturzertifikates hat („sole control“ oder SCAL). Mit SCAL2 wird eine alleinige Zugriffskontrolle basierend auf 2 Faktoren beschrieben, mit SCAL1 eine Zugriffskontrolle mit einem Faktor. Mit der Signaturfreigabe bekundet der Signierende seinen Willen zur Signatur.
Signierender	Natürliche Person, die bei vorgängiger Identifikation und Signaturfreigabe ein Dokument elektronisch signiert.
Signing Service	Teil des Services, der basierend auf den Standard ETSI EN 119 432 die Signatur, das Siegel oder den Zeitstempel auf den Hash eines Dokumentes aufbringt, sofern die Anfrage hierzu auf einem Access Token basiert, welches der Smart Registration Service über den Multiplen Authentication Broker bereitgestellt hat.

Begriff	Beschreibung
Smart Registration Service	Service von Swisscom Trust Services, der die Signaturfreigabe steuert und verwaltet, sowie die Evidenzen archiviert und Informationen über die Signaturfreigabe und Registrierung aus der RA-Datenbank bereitstellt. Nach aussenhin kommuniziert der Smart Registration Service über den Multiplen Authentication Broker und über die Import Schnittstelle der RA Datenbank. Im Rahmen der Signatur bietet der Smart Registration Service die regulatorisch passenden Signaturfreigabemethode an und optional auch die passenden Registrierungsverfahren, sofern ein Signierender nicht registriert ist. Er greift dabei auch auf externe IdP und Services zurück. Historisch bedingt gibt es für Mobilnummer gestützte Signaturfreigabemethode auch eine direkte SRS-Schnittstelle. Über die Kommunikation mit dem Multiplen Authentication Broker wird für Personensignaturen das Access Token für die Signaturanfrage am Signing Service zur Verfügung gestellt.
Store (Registrierungsmethoden oder Signaturfreigabemethoden)	Im Laufe des Signaturworkflow können – optional - im Rahmen eines Webview die verschiedenen regulatorisch passenden Möglichkeiten für eine Signaturfreigabe und/oder Registrierung angeboten werden, sofern diese nicht schon vorab bekannt sind. Die Auswahl erfolgt in einem von Swisscom Trust Services angebotenen Fenster («Store») im Rahmen eines Webviews.
SSL/TLS	Secure Socket Layer, Transport Layer Security, Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet basierend auf SSL (Zugangs-) Zertifikaten
TAV	Technisch Administrative Vorschriften zum Signaturgesetz ZertES der Schweiz.
Teilnehmer	Swisscom Trust Services erbringt die Leistungen gemäss vorliegender Leistungsbeschreibung zu Gunsten des Teilnehmers. Der Teilnehmer ist entweder direkt Kunde von Swisscom Trust Services mit einem Signing Service Vertrag (inklusive Annahmeerklärung gegenüber Swisscom (Schweiz) AG) oder er hat einen kommerziellen Vertrag mit einem Wiederverkäufer der Swisscom Trust Services Leistung mit einer Annahmeerklärung gegenüber Swisscom (Schweiz) AG. Sofern im Falle von Siegelapplikationen aufgrund der fehlenden Einzelsignaturfreigaben der Teilnehmer nicht identisch mit dem Siegelersteller ist, benötigt der Teilnehmer eine Autorisierung dadurch, dass der Siegelersteller das Zugangszertifikat Swisscom Trust Services elektronisch zusendet oder übergibt, oder das vom Teilnehmer autorisierte Zugangszertifikat Swisscom Trust Services gegenüber akzeptiert.
Teilnehmerapplikation	Der Teilnehmer gibt den Signierenden und Signaturerstellern Zugang zu einer Applikation, mit der sie elektronische Signaturen, Siegel und Zeitstempel gemäss den Nutzungsbestimmungen von Swisscom (Schweiz) AG bzw. Swisscom ITSF erstellen können und der Teilnehmer stellt dabei neben der Authentisierung die Übertragung der Signaturdaten zum Fernsignaturservice der Swisscom Zertifizierungs- und Vertrauensdienste sicher ("Teilnehmerapplikation"). Die Teilnehmerapplikation nimmt die signierten Daten (Hash) entgegen und bereitet für den Signierenden das Dokument auf. Der Smart Registration & Signing Service bietet eine Schnittstelle, die mit einer Teilnehmerapplikation zur Auslösung der Signatur verbunden wird. Die Teilnehmerapplikation ist nicht Bestandteil dieser Leistungsbeschreibung, sie wird ausserhalb des Signing Service z.B. durch Partner bereitgestellt.
Token	Siehe Access Token.
UID-Einheit	Organisation gemäss Art. 3 Abs. 1 Bst. c UIDG, der eine Unternehmens-Identifikationsnummer (UID) zur eindeutigen Identifizierung zugeordnet wurde. Nur UID-Einheiten können Ersteller für elektronische Siegel der Schweiz gemäss CP/CPS sein.
UIDG	Schweizerisches Bundesgesetz vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer
Umsetzungskonzept	Im Falle von kundeneigenen Identifikationsmethoden für die Registrierung oder im Falle der Verwendung kundeneigener Signaturfreigabemethoden für die Signaturfreigabe müssen diese Methoden und weitere regulatorisch relevante Punkte in einem Umsetzungskonzept beschrieben und von Swisscom Trust Services freigegeben werden. Das Umsetzungskonzept dient auch als Grundlage für die Beantragung des Audits dieser Methoden.

Begriff	Beschreibung
UUID	Ein Universally Unique Identifier (UUID) ist eine 128-Bit-Zahl, welche zur Identifikation in Computersystemen verwendet wird. Er wird von Swisscom Trust Services als Identifikator für die Zugangszertifikate verwendet.
Vertrauensdienst	In der eIDAS Verordnung verwendeter Begriff für den Anbieter von vertrauenswürdigen Signaturen, Siegel und Zeitstempel sowie Zertifikaten. Im Schweizer Signaturgesetz wird analog der Begriff der «Anbieterin von Zertifizierungsdiensten» gebraucht.
Webauthn	WebAuthn ist ein vom World Wide Web Consortium (W3C) im Rahmen des FIDO2-Standards veröffentlichter Einzelstandard für eine Programmierschnittstelle (API), mit der Webanwendungen und Websites ihren Benutzern eine direkte Authentifikation mittels Public-Key-Verfahren (Passkey) im Webbrowser anbieten können.
Webview	Mit Hilfe eins Webviews wird eine Ansicht gezeigt oder in einer App/Anwendung eingebettet, die Webinhalte – in diesem Fall von Swisscom Trust Services – anzeigt.
X.509	X.509 ist ein Standard der ITU-T für die Erstellung digitaler Zertifikate und spezifiziert den Zertifikatsaufbau.
Zeitstempel	Bestätigung, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorliegen. Der Aufbau des Zeitstempels richtet sich nach RFC 3161.
ZertES	Schweizerisches Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate
Zertifikat	Das Zertifikat ordnet den öffentlichen Schlüssel einem Inhaber zu, z.B. einem Signierenden oder einem Siegelersteller zu. Ein Zertifizierungs- oder Vertrauensdienst überprüft den Inhaber und signiert diese Zuordnung. Das Zertifikat ist einem Wurzelzertifikat zugeordnet, welches dem Zertifizierungs- oder Vertrauensdienst gehört und in allen Validierungen als vertrauenswürdig eingestuft wird.
Zertifizierungsdienst	Im Schweizer Signaturgesetz ZertES genutzter Begriff für Bereitstellung von Signaturen, Siegel, Zeitstempel inklusive der Zertifikate. Der Vertrauensdienst ist dabei der Anbieter von Zertifizierungsdiensten.
Zugangszertifikat	Zertifikat, welches einerseits den Zugang der Teilnehmerapplikation zum Signing Service und Multiple Authentication Broker authentisiert und andererseits zur verschlüsselten Kommunikation mit dem Signing Service und dem Multiplen Authentication Broker dient. Es handelt sich um ein von Swisscom Trust Services aufgrund einer vom Teilnehmer übergebenen Zertifikatsanforderung (CSR) erstelltes SSL/TLS-Zugangszertifikat mit einer eindeutigen Kennung (UUID). Der Teilnehmer hat hierfür den privaten Schlüssel. Die Spezifikation ist in der Annahmeerklärung enthalten. Im Falle einer Siegelapplikation aufgrund der fehlenden Einzelsignaturfreigabe braucht es im Falle, dass Teilnehmer und Siegelersteller nicht identisch sind, zusätzlich zur Übergabe des Zugangszertifikats an Swisscom Trust Services auch eine schriftliche Genehmigung des Siegelerstellers, welche die Verwendung des Zugangszertifikats zur Erstellung elektronischer Siegel im Namen des Siegelerstellers über die Teilnehmerapplikation des Teilnehmers gegenüber Swisscom (Schweiz) AG bzw. Swisscom ITSF zulässt. Im Falle eines geregelten Zertifikates behält der Siegelersteller immer den Zugriff auf den privaten Schlüssel dieses Zugangszertifikates und übergibt dieses persönlich an einen Vertreter des jeweiligen Swisscom Zertifizierungs- oder Vertrauensdienstes.

4 Ausprägungen und Optionen

Die Store Registrierungsmethoden, Signaturfreigaben und die Einbindung von kundeneigenen Registrierungs- und Signaturfreigabemethoden sind in der "Leistungsbeschreibung Registrierungs- und Signaturfreigabemethoden" beschrieben. Die Registrierung via RA-App ist in der "Leistungsbeschreibung RA-App" beschrieben.

Standardausprägung	Elektronische Personensignaturen
Plattform zum Bezug von Identifikationen, Signaturfreigabemethoden und elektronischen Signaturen, Siegeln oder Zeitstempel	●
Personensignatur: Qualifizierte elektronische Signatur ZertES (CH)	○
Personensignatur: Fortgeschrittene elektronische Signatur für die Schweiz (CH)	○
Qualifizierter elektronischer Zeitstempel ZertES/eIDAS (CH/EU)	○
Geregeltes Siegel ZertES (CH)	○
Fortgeschrittenes Siegel für die Schweiz (CH)	○
Behördensiegel für die Schweiz (CH)	○
Personensignatur: Qualifizierte elektronische Signatur eIDAS (EU)	○
Personensignatur: Fortgeschrittene elektronische Signatur eIDAS (EU)	○
Qualifiziertes Siegel eIDAS (EU)	○
Fortgeschrittenes Siegel eIDAS (EU)	○
Registrierungen in ausgewählten Swisscom Shops	●
Registrierungen mit der RA-App	○
Zugang zum Store Registrierungsmethoden und Signaturfreigaben	●
Datenaufbewahrung in der Schweiz	●
Betrieb und Ausstellung aller Zertifikate, Signaturen, Siegel und Zeitstempel gemäss Zertifikatsrichtlinien (CP/CPS)	●
Nutzung für Signierende mit Wohnsitz in Schweiz, EU und EWR	●
Nutzung für Signierende mit Wohnsitz ausserhalb Schweiz, EU und EWR	○
Haftungsbeschränkungen in den Zertifikaten	○

● = Standard (im Preis inbegriffen) ○ = Gegen Aufpreis

4.1 Definition der Leistungen

Leistung	Definition
Plattform zum Bezug von Identifikationen, Signaturfreigabemethoden und elektronischen Signaturen, Siegeln oder Zeitstempel	Mit dem Zugang zu der Registration Service & Signing Service Plattform erhalten Teilnehmer die Möglichkeit Signaturen, Siegel und/oder Zeitstempel für einen Hash eines Dokumentes zu beziehen. Diese müssen jeweils in der Bestellung bestellt werden. Für eine Signatur muss der Signierende zur Freigabe der Signatur registriert sein. Die Plattform bietet Zugang zu verschiedenen Identifikationsmöglichkeiten und Signaturfreigabemethoden. Diese können ebenfalls im Bestellformular einzeln ausgewählt und bestellt werden und sind in der Leistungsbeschreibung zu den Registrierungs- und Signaturfreigabemethoden beschrieben. Darüber hinaus ist im Zusammenhang mit der Leistung «Onboarding Support» auch der Einbezug von eigenen Identifikationsverfahren und Freigabelösungen möglich Hierbei wird in der Regel ein Audit sowie zusätzliche Projekt- und Beratungsleistungen notwendig sein. Der Multiple Authentication Broker koordiniert den Ablauf der Registrierung und Signaturfreigabe im Vorfeld der Signatur. Die Signaturapplikation kommuniziert somit zuerst mit dem Multiple Authentication Broker und erhält über das OpenID Connect (OIDC) Protokoll den Authorization Code und erwirbt über diesen das Zugangstoken zum Signing Service für die Hash Signatur.
Personensignatur: Qualifizierte elektronische Signatur ZertES (CH)	Qualifizierte elektronische Signatur gemäss Art. 2 Bst. e ZertES.
Personensignatur: Fortgeschrittene elektronische Signatur für die Schweiz (CH)	Fortgeschrittene elektronische Signatur gemäss ETSI-Standard 319 411 "NCP+" und gemäss CP/CPS des Zertifizierungsdienstes der Swisscom (Schweiz) AG, Schweiz.
Qualifizierter elektronischer Zeitstempel ZertES/eIDAS (CH/EU)	Qualifizierter elektronischer Zeitstempel gemäss Art. 2 Bst. j ZertES und gemäss Art. 3 Ziff. 34 eIDAS-VO. Grundsätzlich ist bei allen Signaturen und

Leistung	Definition
	Siegeln, sofern nicht anders angegeben, ein qualifizierter elektronischer Zeitstempel immer inbegriffen.
Geregeltes Siegel ZertES (CH)	Geregeltes elektronische Siegel gemäss Art. 2 Bst. d ZertES: eine fortgeschrittene elektronische Signatur, die unter Verwendung einer sicheren Siegelerstellungseinheit nach Artikel 6 ZertES erstellt wurde und auf einem geregelten und zum Zeitpunkt der Erzeugung des elektronischen Siegels gültigen Zertifikat beruht. Die Siegelzertifikate können ausschliesslich im Namen einer UID-Einheit ausgestellt werden.
Fortgeschrittenes Siegel für die Schweiz (CH)	Fortgeschrittenes elektronisches Siegel gemäss ETSI-Standard 319 411 "NCP+"
Behördensiegel (CH)	Behördensiegel sind geregelte Siegelzertifikate, die gemäss den "Technisch Administrativen Vorschriften" (TAV) zum ZertES vom 15.3.2022 für Behörden ausgestellt werden. Diese werden von Swisscom (Schweiz) AG mit den in Kapitel 2.3.4 a) der TAV spezifizierten Vorschriften zu den Behördenbezeichnungen in den OU-Feldern ausgestellt, allerdings ohne das optionale Feld businessCategorie gemäss 2.3.4 b) der TAV.
Personensignatur: Qualifizierte elektronische Signatur eIDAS (EU)	Qualifizierte elektronische Signatur gemäss Art. 3 Ziff. 12 eIDAS-VO.
Personensignatur: Fortgeschrittene elektronische Signatur eIDAS (EU)	Fortgeschrittene elektronische Signatur gemäss ETSI-Standard 319 411 "NCP+" und gemäss Art. 3 Ziff. 11 eIDAS-VO.
Fortgeschrittenes Siegel eIDAS (EU)	Fortgeschrittenes elektronisches Siegel gemäss Art. 3 Ziff. 26 eIDAS-VO und gemäss ETSI-Standard 319 411 "NCP+"
Qualifiziertes Siegel eIDAS (EU)	Qualifiziertes elektronisches Siegel gemäss Art. 3 Ziff. 27 eIDAS-VO. Dieses kann ausschliesslich im Namen einer juristischen Person im Sinn der eIDAS-VO ausgestellt werden.
Registrierungen mit der RA-App	Die RA-App ist eine App, die es Personen einer RA-Agentur ermöglicht, face2face Identifikationen durchzuführen. Die RA-Agentur kann z.B. auch der Teilnehmer selber sein und muss einen Vertrag mit den Swisscom Trust Services abschliessen. Weitere Einzelheiten können der separaten Leistungsbeschreibung "RA-App" entnommen werden.
Registrierungen in ausgewählten Swisscom Shops	In ausgewählten Swisscom Shops (siehe Übersicht auf https://srsident.trustservices.swisscom.com) der Schweiz kann sich ein zukünftig Signierender kostenfrei im face2face Verfahren identifizieren lassen und folgende Signaturfreigabemethoden registrieren lassen: • Mobile ID App • Mobile ID auf Schweizer SIM-Karte • Passwort in Kombination mit Einmalcode via SMS Hierzu muss vor der Registrierung die Mobile ID App installiert sein oder die Mobile ID auf der Schweizer SIM-Karte unter mobileid.ch aktiviert sein. Der zukünftig Signierende erhält nach der Registrierung auf seinem Smartphone unter der während der Registrierung angegebenen Mobilnummer eine SMS mit Links zu den Nutzungsbestimmungen der Swisscom Zertifizierungs- und Vertrauensdienste und muss diese mit einer Signaturfreigabemethode bestätigen. Danach kann er die gewählte Signaturfreigabemethode für alle Signaturen verwenden bis zum Ablauf der Gültigkeit seines Ausweisdokumentes oder längstens 5 Jahre. Die Signaturfreigabemethoden sind in der Leistungsbeschreibung zu den Registrierungs- und Signaturfreigabemethoden beschrieben. Weitere Signaturfreigabemethoden und Identifikationsmethoden werden laufend aufgeschaltet.
Zugang zum Store Fernregistrierungsmethoden und Signaturfreigaben	Swisscom Trust Services bietet über den Multiple Authentication Broker (MAB) verschiedene remote Identifikations- und Signaturfreigabemethoden im sogenannten Storekonzept an. D.h. im Rahmen einer Signaturapplikation kann die Berechtigung zur Nutzung von bestellte Identifikationsverfahren und Signaturfreigabemethoden konfiguriert werden. Hierbei kann eine regelmässige Bereitstellungsgebühr entfallen gemäss dem Bestellformular. Zuzüglich können auch Nutzungsgebühren vom Teilnehmer erhoben werden, der diesen Store in seinen Signaturfluss einbettet. Im Store werden sowohl Angebot der Swisscom Trust Services bereitgestellt wie z.B. die Mobile ID,

Leistung	Definition
	Mobile ID App, das Passwort/Einmalcode Freigabeverfahren oder eine Signaturfreigabe App als auch Angebote Dritter, z.B. Passkeys/FIDO2 oder Apps ausgewählter IdPs. Hierbei werden die Leistungen Dritter durch die Swisscom Trust Services wiederverkauft. Die Services sind in gesonderten Leistungsbeschreibungen beschrieben und unterliegen eigenen SLA und Mitwirkungsanforderungen. Swisscom Trust Services bietet im Rahmen des Storekonzeptes an, dass auditierte und freigegebene IdPs und Identitätsprüfer sowie Signaturfreigabemethode der Teilnehmer ebenfalls wiederverkauft werden. Swisscom Trust Services erhebt als Wiederverkäufer auf die angebotenen Einkaufspreise eine Support- und Servicegebühr. Das Storekonzept ist in der Leistungsbeschreibung zu den Registrierungs- und Signaturfreigabemethoden beschrieben.
Datenaufbewahrung in der Schweiz	Die Datenaufbewahrung der Personendaten aus den Zertifikaten und der an Swisscom Trust Services übermittelten Evidenzen findet nur in der Schweiz im Einklang mit den einschlägigen Vorschriften der schweizerischen Datenschutzgesetzgebung und unter Einhaltung der DSGVO der EU bzw. der DSG der Schweiz statt. Die Datenverarbeitung durch die teilweise von Partnern bereitgestellte Registrierungs- und/oder Signaturfreigabemethoden kann – je nach Typ – auch im Ausland stattfinden. Die Mobile ID und Passwort Verarbeitung findet nur auf Schweizer Servern statt. Die SMS mit dem Einmalcode wird aus der Schweiz oder der EU versendet.
Betrieb und Ausstellung aller Zertifikate, Signaturen, Siegel und Zeitstempel gemäss Zertifikatsrichtlinien (CP/CPS)	Der Betrieb eines Zertifizierungsdiensteanbieters der Schweiz bzw. des Vertrauensdienstanbieters der EU und die Ausstellung der betreffenden Zertifikate, Signaturen, Siegel und Zeitstempel richtet sich nach den Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten der Klasse "Diamant“ (qualifiziert) und „Saphir“ (fortgeschritten) im jeweiligen Rechtsraum Schweiz oder EU/EWR. Diese können in der aktuellen Fassung hier aufgerufen werden: **https://trustservices.swisscom.com/repository/**
Nutzung für Signierende mit Wohnsitz in Schweiz, EU und EWR	Die Nutzungsbestimmungen genügen rechtlich nur den Anforderungen für Signierende mit Wohnsitz in der Schweiz, EU und EWR. Damit richtet sich der Service ohne Bestellung von Zusatzoptionen nur an Signierende mit Wohnsitz in diesen Staaten.
Nutzung für Signierende mit Wohnsitz ausserhalb der Schweiz, EU und EWR	Auf Grund von ggfs. länderspezifischen rechtlichen Anforderungen können die derzeit vorhandenen Nutzungsbestimmungen für Signierende mit Wohnsitz ausserhalb der Schweiz, EU und EWR nicht verwendet werden. Es besteht das Risiko der Ungültigkeit der ausgestellten Signatur. Sofern der Service auch Signierenden ausserhalb der Schweiz, EU und EWR zugänglich gemacht werden soll, muss das rechtlich und technisch (z.B in Bezug auf die Nutzung der Signaturfreigabemethode und der Verschlüsselungsanforderungen) geprüft werden. Ggfs. müssen die Nutzungsbestimmungen aufgrund der konsumentenrechtlichen Reglungen dafür angepasst werden und die technischen Signaturfreigabemöglichkeiten überprüft und bereitgestellt werden. Das ist nach Absprache und gegen gesondertes Angebot der Swisscom Trust Services möglich.
Haftungsbeschränkung in den Zertifikaten	Es besteht die Möglichkeit, Zertifikate mit Haftungsobergrenze im Sinne von Art. 13 (2) eIDAS oder Art. 7 Abs. 3 Bst. c und d ZertES auszustellen. In diesem Fall zeigt das Zertifikat die Haftungsobergrenze als Parameter „QcEuLimitValue“ in EUR an. Die Haftungsbeschränkung findet nur auf besondere Anforderung statt bzw. für Signaturen, die für Signierende mit Wohnsitz ausserhalb der EU/EWR und Schweiz ausgestellt werden.

4.2 Zertifikatsinhalte

4.2.1 Personensignaturen

Personensignaturen enthalten folgende Informationen im Zertifikat (Distinguished Name):

Common name= <Vorname, Name des Signierenden>

givenname= <Vorname(n) gemäss Ausweisdokument>

surname= <Nachname(n) gemäss Ausweisdokument>

country= <Wohnsitzland oder Heimatland des Signierenden >
serialnumber= < evidence ID des RA Service oder andere Seriennummer im Falle einer eigenen Identifikation >

Alternativ können auch pseudonymisierte Zertifikate ausgestellt werden:
Common name= <Vorname, Name des Signierenden> ODER PSEUDONYM:<andere Information in Bezug auf den Signierenden>
pseudonym= <Mobilfunknummer im internationalen Format oder evidenceID (siehe unten)>
country= <Wohnsitzland oder Heimatland des Signierenden>
serialnumber= < evidenceID des RA Service nach verify Aufruf oder andere Seriennummer im Falle einer eigenen Identifikation >

Es gilt zu beachten, dass Validatoren Warnmeldungen im Falle von pseudonymisierten Zertifikaten ausgeben.

In der Leistungsbeschreibung zu den Registrierungs- und Signaturfreigabeverfahren wird das Fasttrack Verfahren beschrieben, welches die Freigabe von fortgeschrittenen elektronischen Signaturen ohne vorgängige Registrierung über eine in der Schweiz registrierte Mobilnummer erlaubt und den gesetzlichen Identifikationszwang bei der SIM Ausgabe in der Schweiz nutzt. Fasttrack Zertifikate (Schweiz/FES) enthalten folgende Inhalte:
Common name = <Mobiltelefonnummer des Signierenden mit Präfix "417">
pseudonym= <Mobiltelefonnummer des Signierenden mit Präfix "417">
country = "CH"
serialnumber= <Aktuelles Datum im Format YYYYMMDD>-<Mobiltelefonnummer des Signierenden mit Präfix "417">

4.2.2 Siegel

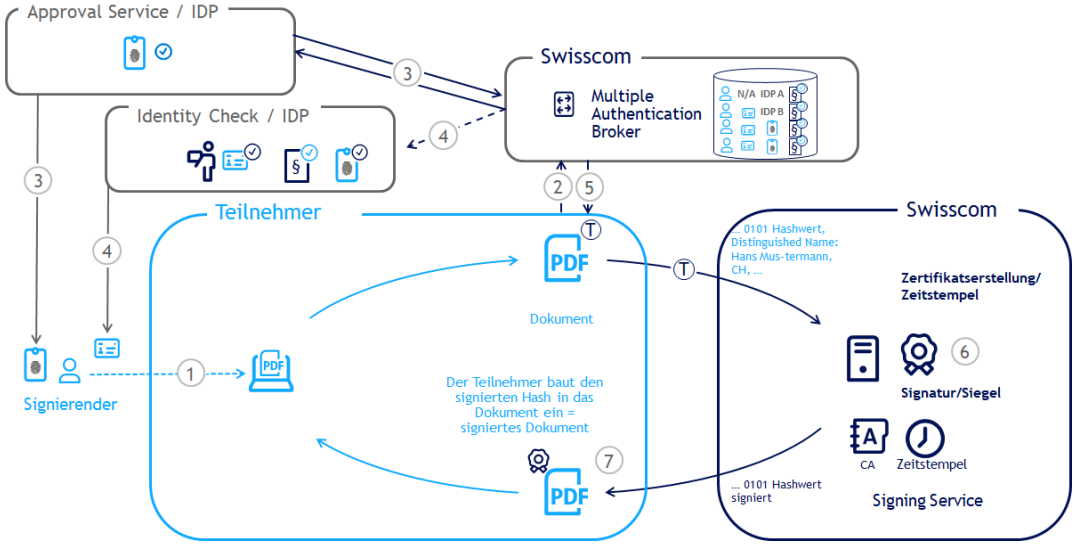
Siegel enthalten folgende Inhalte:
Common name: <Bezeichnung des Siegels gemäss Antrag durch den Teilnehmer>
Organization: <Genaue Bezeichnung gemäss Handelsregister, UUID-Register, ESTV, etc.>
Organizational Unit:<Abteilung oder Funktion innerhalb der Organisation (optional)– oder Bezeichner im Rahmen Behördenzertifikat. Es darf kein Organisationsname einer anderen Organisation verwendet werden.>
Country: <Niederlassungsland der Organisation, bzw. Land in dem das Register geführt wird>
Locality: <Stadt oder Gemeinde, in der die Organisation ihren Sitz hat (optional)
State: <Kanton, Bundesland etc. in der die Organisation ihren Sitz hat (optional)
organizationIdentifier: <Schweiz: UUID – EU: Registerkennung und Registernummer>

4.3 Ablauf der Signaturerstellung für alle Optionen

Die Teilnehmerapplikation hat im Wesentlichen zwei Endpunkte:

- Multi Authentication Broker: Dieser nimmt die Signaturanfragen entgegen und prüft die Signaturfreigabe mit der bei der Registrierung hinterlegten Signaturfreigabemethode. Gegebenenfalls bietet er eine Registrierung mit einem der angebotenen Verfahren des Registrierungsstores an, sofern der Signierende bisher noch nicht registriert wurde. Gemäss dem Open ID Connect Standard Protokoll vergibt der Multi-Authentication Broker ein Authenticationcode und damit ein Zugangstoken für den Signing Service.
- Siging Service: Auf Basis des Zugangstokens kann die Teilnehmerapplikation eine Signaturanfrage stellen und gibt den Dokumentenhash mit zur Signatur. Der Hash wird signiert zurückgegeben und muss in der Signaturapplikation nun wieder zu einem vollständigen signierten Dokument (z.B. PDF) zusammengebaut werden.

Registrierungen können entweder vorab z.B. durch einen Shopbesuch, mit der RA-App, über das Registrierungsportal von Swisscom Trust Services oder durch ein Registrierungsportal, welches der Teilnehmer über direkten Zugang zum Smart Registration Service anbietet, geschehen oder die Person wird über die in den Stores verfügbaren Fernidentifikationsmethoden registriert. Die Registrierungs- und Signaturfreigabemethoden sind ein einer eigenen Leistungsbeschreibung beschrieben.



- Ein Signierender möchte ein Dokument signieren (1). Er erhält dieses angezeigt in der Signaturapplikation des Teilnehmers.
- Der Teilnehmer stellt zunächst eine Autorisierungsanfrage beim Multi-Authentication Broker (2). Diese beinhaltet bereits den Hash der zu signierenden Dokumente, sowie den Rechtsraum und die Signaturart (FES/QES), sowie ggfs. weitere Ablaufparameter. Das Swisscom System schaut in der Swisscom RA Datenbank nach, welche Signaturfreigabemethode vom Signierenden während der Registrierung hinterlegt wurde. Das kann auch von einem delegierten Dienst angeboten werden (z.B. ein IdP), der die Signaturfreigabe mit seinem eigenen Authentisierungsmittel sicherstellt. Hierfür kann die Teilnehmerapplikation einen Hinweis («login_hint» für z.B. eine E-Mail/Mobilnummer oder «IdP_hint» für einen IdP) mitgeben. Ist kein Hinweis vorhanden, wird der Signierende angefragt, die während der Registrierung hinterlegte Signaturfreigabemethode auszuwählen.
- Der Multi Authentication Broker stellt nun eine Verbindung zu dem Signaturfreigabedienst her (3), das kann ein interner Dienst sein, wie z.B. Mobile ID oder ein delegierter Dienst eines Partners, ein allgemeiner Dienst wie passkey/FIDO2 (z.B. via webauthn Protokoll) oder externen IdP, z.B. einer Bank. Während dieses OAuth Authentication Request Calls muss der Signierende die Signaturfreigabe einleiten, z.B. durch Freigabe mit einem Fingerprint in einer Freigabeapp. Für qualifizierte/geregelte Signaturzertifikate ist eine 2-Faktor Signaturfreigabe notwendig, für fortgeschrittene Signaturen reicht auch eine 1-Faktor Signaturfreigabe. Es wird überprüft, ob der Nutzer bereits mit dieser registriert war. Falls die Freigabeautorisierung fehlgeschlagen ist, gibt es maximal 5 Versuche. Danach muss der Nutzer sich neu registrieren lassen.
- Im Falle, dass der Signierende noch nicht registriert wurde, wird ein Identifikationsverfahren oder IdP zur Registrierung passend zum Rechtsgebiet, dem Signaturniveau (FES/QES) und der ausgewählten Signaturfreigabemethode angeboten. Sofern nicht anders konfiguriert, wird hierzu im Signaturfluss ein "Store" aufgeschaltet, in dem verschiedene Registrierungsmöglichkeiten angeboten werden (siehe separate Leistungsbeschreibung). Der ausgewählte Identifikationsservice wird vom Swisscom System aufgefordert die Identifikation durchzuführen (4). Die Registrierung besteht immer aus den Schritten:
    - Identifikationsprüfung bzw. Feststellen der Identität
    - Verwendung der Signaturfreigabemethode
    - Akzeptanz der Nutzungsbestimmungen für den Signaturservice des Swisscom Zertifizierungs- und Vertrauensdienstes.

  Im Falle eines IdP wird typischerweise auf bereits vorhandene Identitäten zurückgegriffen, d.h. es erfolgt dann eine Authentifizierung gegenüber dem IdP. Diese Authentifizierungsmethode wird später auch für die Freigabe für die Signaturen verwendet. Es ist lediglich noch die Akzeptanz der Nutzungsbestimmungen notwendig.
- Sollte die Signaturfreigabe – ggfs. nach erfolgter Registrierung - in Ordnung sein, wird vom Swisscom Multiple Authentication Broker der Teilnehmerapplikation ein Authorization Code zurückgegeben, mit dem nun die Signaturapplikation das Zugangstoken (Access Token (T)) für die Signatur anfragen kann (5).
- Die Teilnehmerapplikation fordert nun mit dem Token (T) beim Signing Service eine Signatur an. Das Protokoll basiert auf ETSI EN 119 432 Standard für Fernsignaturen. Zu den Swisscom Systemen wird nur der Hash eines Dokumentes übermittelt und nicht das gesamte Dokument. Der Signaturservice gibt sofort den signierten Hash zurück. Ebenfalls kann die Teilnehmerapplikation auch einen Zeitstempel beziehen. (6) Beides kann kombiniert mit Informationen zur Zertifikatskette bis hin zum vertrauenswürdigen Wurzelzertifikat und Informationen zum Widerrufstatus der

Zertifikate in das Dokument eingebaut werden und somit ein Langzeit-Validierbares signiertes Dokument erstellt werden (LTV). (7)

Für Personensignaturen verwendet der Swisscom Zertifizierungs- bzw. Vertrauensdienst in der Regel ein Kurzzeitzertifikat, welches nur gültig für die jeweilige Signaturanfrage ist. Das zugehörige Schlüsselpaar wird hierfür kurzzeitig erstellt und danach gelöscht.

Siegel basieren in der Regel auf Langzeitzertifikaten, die auf eine Organisation ausgestellt werden. Die Signaturfreigabe kann bei Organisationen auch dauerhaft ohne Einzelfreigabe geschehen, z.B. über eine dauerhafte zertifikatsbasierte Freigabe, wobei der private Schlüssel vom Verantwortlichen der Organisation verwaltet wird. Diesbezüglich ist immer ein Dokument zu den Einsatzbedingungen für die Siegelerstellung mit Swisscom Trust Services zu vereinbaren, wie die dauerhafte Freigabe regulatorisch und gesetzlich konform durchgeführt werden kann. Hierbei sind insbesondere die Anforderungen nach CEN/TS 419 241-1 zu beachten.

Zeitstempel richten sich in der Struktur nach RFC3161, hingegen wird das RFC3161 Protokoll zur Ausstellung von Zeitstempel nicht befolgt.

In eine Anfrage können auch Batches von Signaturen verarbeitet werden (maximal 250 Hashes können mitgegeben werden). Im Signaturzertifikat wird der Name, Vorname, Land und eine Seriennummer angegeben oder anstelle des Namens und Vornamens ein Pseudonym. In der Regel stellt der Signing Service den Zertifikatsinhalt aus den Angaben des IdP bzw. der RA-Datenbank zusammen.
Der signierte Hashwert wird im CMS oder PCKS#1 Standard zurückgegeben.

Der Ablauf oben kann auch variieren durch Ablaufparameter, die mitgegeben werden. So ist es möglich, z.B. einen one-shot Prozess zu initiieren, der ohne Signaturfreigabemittel eine Signaturfreigabe nur durch Identifikation ermöglicht.

4.4 Prozesse und Tools zur Personenidentifikation (Registrierungsstelle)

Bevor eine Signaturfreigabe möglich ist, muss der Signierende sich entsprechend den Anforderungen der jeweiligen Art der elektronischen Signatur identifizieren und registrieren. Der Identifikationsprozess kann losgelöst vom Signaturprozess durch eine sogenannte Registrierungsstelle erfolgen. Swisscom Trust Services bietet hierfür mehrere Varianten an:

- Der Teilnehmer kann in die Lage versetzt werden, für die Swisscom Zertifizierungs- und Vertrauensdienste lokal selbst Kollegen, Kunden und Partner im face2face Verfahren zu identifizieren. Hierfür kann er die Swisscom RA-App einsetzen. Diese ist gesondert zu bestellen und in der Leistungsbeschreibung RA-App beschrieben.
- Der Teilnehmer kann ein online Identifikationsverfahren nutzen, welches ein Partner im Rahmen von Smart Registration Service als Fernidentifikationsverfahren auf einem eigenen Registrierungsportal anbietet. Diese werden in der Leistungsbeschreibung zu den Registrierungs- und Signaturfreigabemethoden beschrieben und müssen gesondert bestellt werden.
- Swisscom Trust Services bietet online Registrierungsmöglichkeiten auch direkt zum Bezug über Gutscheincodes oder Direktbezahlung über das eigene Registrierungsportal https://srsident.trustservices.swisscom.com an. Diese Verfahren sind ebenfalls in der Leistungsbeschreibung zu den Registrierungs- und Signaturfreigabemethoden beschrieben.
- Innerhalb des Signaturflusses stellt der Multiple Authentication Broker fest, wenn eine Person nicht registriert ist und bietet dann direkt über einen sogenannten "Store" verschiedene online Registrierungsmöglichkeiten an. Die Möglichkeiten können teilnehmerspezifisch konfiguriert werden und die Nutzung unterliegt zusätzlichen Kosten gemäss Bestellformular oder Vertrag. Hierzu wird ebenfalls auf die Leistungsbeschreibung zu den Registrierungs- und Signaturfreigabemethoden verwiesen.
- IdPs können ihren Nutzern oder über den Smart Registration Service ebenfalls Registrierungen mit Authentifizierungsmittel anbieten, die auch in anderen Signaturapplikationen zur Willensbekundung eingesetzt werden. Diese Verfahren werden dann – sofern vom IdP freigegeben - ebenfalls im Store angeboten.
- Der Signierende kann sich andernfalls auch vor Ort in den Swisscom Shops (Face2Face) identifizieren lassen.
- Der Teilnehmer kann seine eigenen Identifikationsmethoden nutzen und selbst eine Registrierungsstelle mit projektspezifischer Identifizierung aufbauen und dabei selbst die Rolle eines IdP einnehmen. Dieses Vorgehen ist vorgängig mit Swisscom Trust Services abzustimmen und im Rahmen eines Signing Onboarding Projektes zu erarbeiten. Hierzu muss der Teilnehmer ein Umsetzungskonzept vorlegen, welches durch Swisscom Trust Services geprüft und bewertet wird. In der Regel müssen für Teilnehmer individualisierte Registrierungsstellenprozesse zusätzlich von der Anerkennungsstelle oder Konformitätsbewertungsstelle für Zertifizierungsdienste oder Vertrauensdienste freigegeben werden. Die Registrierungsdaten können je nach Ausprägung beim Teilnehmer verbleiben oder auch in den Swisscom Smart Registration Service transferiert werden. Hierzu ist eine gesonderte Bestellung notwendig. Der Prozess ist in der Leistungsbeschreibung Onboarding Support beschrieben.

Daten der eigenen Identifikationsmethode bzw. des IdP werden an Swisscom als Evidenz bereitgestellt und von Swisscom in der RA Datenbank verwaltet. Es ist möglich, dass nur eine Archivierung der Referenz dieser Daten erfolgt

und der eigentliche Datensatz dann beim Identifizierer verbleibt. Diese Aufbewahrung der Daten muss dann entsprechend auditiert werden und im Rahmen des Onboarding Supports beauftragt werden. Eine Evidenz umfasst:

- Einsatz in Bezug auf die Qualität der Signatur (z.B. fortgeschritten / qualifiziert / geregelt)
- Einsatz in Bezug auf den einsetzbaren Rechtsraum, z.B. Schweiz, EU/EWR, in Abhängigkeit vom zugelassenen Identifikationsverfahrens, des eingesetzten Signaturfreigabemethodes und der akzeptierten Nutzungsbestimmungen
- Einsatz in Bezug auf die erlaubte Gültigkeitsdauer der Evidenz
- Notwendige Signaturfreigabemethode für den Einsatz, sofern nicht ein IdP zuständig ist
- Zuständiger IdP (sofern dieser registriert hat) für die Freigabe der Signatur
- Nachweise über die Identifikation (z.B. ein Photo des Ausweises), je nach Verfahren angepasst.

Die RA Datenbank stellt für die verwalteten Evidenzen auch die notwendigen Angaben für das Zertifikat zusammen: Vorname, Name und Land sowie die Seriennummer.

4.5 Prozess zur Organisationsprüfung

Sofern im Zertifikat eine Organisation benannt werden soll, muss eine Organisationsprüfung gemäss Bestimmung der CP/CPS vor Aufnahme des Service von Swisscom Trust Services durchgeführt werden. Bei Personenzertifikaten muss die Organisation in der Annahmeerklärung benannt sein und ein autorisierter Vertreter der Organisation muss die Annahmeerklärung unterzeichnet haben. Mit der Unterzeichnung gibt er auch eine Freigabe für die Nutzung des Organisationsnamens im Zusammenhang mit den Signierenden.
Im Fall von Siegeln prüft die Registrierungsstelle den Siegelersteller vorab anhand von z.B. Registereinträgen und nimmt einen Antrag eines zeichnungsberechtigten Vertreters des Siegelerstellers entgegen. Dieser muss vor einem von Swisscom Trust Service ernannten Berechtigten persönlich erscheinen (z.B. Identifikation mittels RA-App). Im Falle von Unterschriftsregelungen durch zwei Zeichnungsberechtigte muss noch ein weiterer Vertreter des Siegelerstellers mitunterzeichnen. Der Antrag und weitere eingereichte Unterlagen werden geprüft und archiviert. Die Unterschriften muss qualifiziert elektronisch erfolgen und mit einem Mobile ID oder Passwort/Einmalcodeverfahren freigegeben worden sein. Die dort verwendete Rufnummer ermöglicht mit Mobile ID bzw. Passwort/Einmalcode den Widerruf des Siegelzertifikates im Falle einer Kompromittierung (siehe unten) .
Nach Genehmigung des Antrags wird für den Siegelersteller das Schlüsselmaterial auf der Signing Service Plattform erzeugt und hinterlegt. Zu diesem Schlüsselpaar wird ein entsprechendes Langzeit-Siegelzertifikat (in der Regel 3 Jahre) gemäss den Zertifikatsrichtlinien der Swisscom (Schweiz) AG bzw. der Swisscom ITSF und dem im Siegelzertifikatsantrag benannten Subjekt des Siegelzertifikates (Distinguished Name des Siegelerstellers) ausgestellt.

4.6 Revokation (Ungültigkeitserklärung) eines Siegel- und/oder Zugangszertifikates

Siegel- und zugehörige Zugangszertifikate müssen vom Siegelersteller als ungültig erklärt werden, sofern Anzeichen eines Missbrauches oder Kompromittierung sichtbar werden. Das Swisscom System stellt danach ein neues Siegelzertifikat aus, ggfs. auch auf Basis eines neuen Zugangszertifikates.
Eine Meldung zur Revokation hat durch die im Zertifikatsantrag benannten Vertreter des Siegelerstellers zu erfolgen, deren Authentifizierungsmittel (Mobilnummer) bei Swisscom Trust Services hinterlegt wurde. Diese kann online unter https://trustservices.swisscom.com/repository erfolgen. Ein Revokationsantrag wird mittels der hinterlegten Mobilnummer bzw. der für die persönliche Signatur des Antrages verwendeten Signaturfreigabemittel überprüft. Weitere Verfahren zur Revokation sind gemäss Bestimmungen der CP/CPS möglich.

4.7 Zeitstempel

Zeitstempel benötigen keine Registrierung der Person oder Organisation. Sie basieren auf denselben Schnittstellen wie Signaturen und Siegel und orientieren sich am RFC3161 Standard.

4.8 Prozess zur Prüfung einer Teilnehmerapplikation

Da Swisscom (Schweiz) AG bzw. Swisscom ITSF für die korrekte Ausstellung von Signaturen und Siegeln gegenüber dem Signierenden oder Dritten haftbar ist, erstreckt sich die Verantwortung für die Ausstellung von Signaturen und Siegeln bis auf die korrekte Bearbeitung in der Teilnehmerapplikation. Hierzu muss der Teilnehmer eine Annahmeerklärung unterzeichnen, in denen Pflichten, wie z.B. die Erstellung von TLS/SSL Zugangszertifikaten, Verhinderung des Austauschs eines Dokumentenhash, Schutz der Applikation oder auch Unterzeichnung der Nutzungsbestimmungen im Falle von Siegeln und Zeitstempeldiensten sichergestellt werden.

4.9 Datenablage und Verantwortlichkeiten

Mit der Nutzung der von Swisscom Trust Services zur Verfügung gestellten Registrierungs- und Signaturfreigabemethoden des Smart Registration Service werden die an Swisscom Trust Services übertragenen Daten der identifizierten Person sowie die Identifikationsunterlagen und der Nachweis der Annahme der Nutzungsbestimmungen ausschliesslich auf

Swisscom Servern in der Schweiz gespeichert und entsprechend gemäss den Fristen der CP/CPS oder gemäss Gesetz aufbewahrt. Externe Registrierungsstellen und RA-Agenturen bearbeiten Ihre Daten gemäss der jeweiligen Leistungsbeschreibung der Registrierungs- und Signaturfreigabemethoden bzw. RA-App. Mit Ausnahme der RA-Agenturen sind externe Registrierungsstellen in der Regel eigenständige Datencontroller.
Der Teilnehmer als Bereitsteller der Signaturapplikation ist ebenfalls eigenständiger Datencontroller. Swisscom Trust Services haben mit dem Signierenden durch die Nutzungsbestimmungen ein direktes Vertragsverhältnis und bearbeiten in diesem direkten Verhältnis die Daten der Signierenden. Die Daten des Teilnehmers werden nicht bearbeitet.

5 Leistungsdarstellung und Verantwortlichkeiten

5.1 Signaturservice

Einmalige Leistungen

Tätigkeiten (S = STS/T = Teilnehmer)		S	T
Bereitstellung des Service			
1.	Aufklärung der Signierenden, dass eine Signatur nur nach ordnungsgemässer Registrierung mit einer Signaturfreigabemethode erfolgen kann (z.B. Bestellung einer Registrierung bei Swisscom Trust Services). Es gilt zu beachten, dass nicht alle Nutzer registriert werden können, z.B. aufgrund ungenügender Ausweispapiere, die sich nicht für die maschinelle Registrierung eignen oder einer negativen Risikobeurteilung.		P
2.	Bereitstellung der Signing Service Infrastruktur	P	
3.	Bereitstellung der Schnittstelle SAIP basierend auf ETSI EN 119 432 Standard angepasst für die Nutzung kurzlebiger Signaturzertifikate. Die Schnittstelle ist unter https://documents.swisscom.com/product/filestore/lib/e2007490-6fd4-4012-801d-b104801a9abc/reference_guide_smartregistration_signing-en.pdf?idxme=pex-search abrufbar.	P	
4.	Einhalten der Anforderungen an die regulatorischen Vorgaben bei der Zusammensetzung der Signatur aus dem signierten Hash (z.B. Einhalten des PAdES Standards, Beachtung der Langzeitvalidierung) – siehe hierzu auch den Reference Guide.		P
5.	Zusenden der unterzeichneten Annahmeerklärung mit den regulatorisch notwendigen Informationen.		P
6.	Option "Organisationseintrag im Signaturzertifikat" bei Personenzertifikaten: Bereitstellung auf Anforderung von Swisscom Trust Services aller notwendigen Dokumente zur Organisationsüberprüfung (z.B. beglaubigter Handelsregisterauszug). Unterschrift in der Annahmeerklärung durch einen für die Organisation autorisierter Vertreter zum Einverständnis, dass die Organisation mit der Führung des Organisationsnamens im Zertifikat für die Signierenden einverstanden ist.		P
7.	Option "Organisationseintrag im Signaturzertifikat" bei Personenzertifikaten: Prüfung der Berechtigung zum Führen des Organisationsnamens im Zertifikat.	P	
8.	Option "Siegel": Bereitstellung eines vom Siegelersteller unterzeichneten Antrages zum Siegelzertifikat mit allen notwendigen Dokumenten zur Überprüfung des Siegelerstellers (z.B. beglaubigter Handelsregisterauszug bei geregeltem oder qualifiziertem Siegel) sowie der Zustimmung zu den Nutzungsbestimmungen des Service. Unterschrift im Antrag zum Siegelzertifikat durch einen für den Siegelersteller zeichnungsberechtigten Vertreter. Veranlassung der Identifikation durch persönliches Erscheinen eines Vertreters des Siegelerstellers oder durch qualifizierte elektronische Signatur. Der Teilnehmer stellt sicher, dass der OU-Eintrag (Organizational Unit) im Siegelantrag namensrechtlich nicht mit einer anderen Organisation kollidiert.		P
9.	Option "Siegel": Sicherstellung der Zusendung eines Zugangszertifikates an Swisscom Trust Services durch den Siegelersteller oder dessen Bevollmächtigten mit Bestätigung der Vollmacht.		P
10.	Option "Siegel": Sofern geregelte oder qualifizierte elektronische Siegel erstellt werden, muss ein von Swisscom Trust Services freigegebenes Verfahren zur Signaturfreigabe befolgt werden und in einem Dokument "Einsatzbedingungen für die Siegelerstellung" beschrieben werden. Swisscom Trust Services wird mit dedizierten Partnern ein Verfahren freigeben und einen Vertrag zur "Freigabelösung Siegel" abschliessen.		P
11.	Option "Personensignaturen/Zeitstempel": Zusenden eines CSR für ein SSL/TLS-Zugangszertifikat zur Authentisierung gegenüber dem Multiple Authentication Service und zur verschlüsselten Kommunikation mit dem Signing Service. Spezifikation siehe Annahmeerklärung. Es wird das gleiche Zertifikat verwendet.		P
12.	Option "Personensignaturen": Festlegung und Bestellung der Signaturfreigabemethoden und der Registrierungsmethoden, die während der Signatur ermöglicht werden sollen. Diese werden im "Store" von Swisscom Trust Services konfiguriert (siehe getrennte Leistungsbeschreibung). Der Signierende ist darauf hinzuweisen. Sofern der Signierende nicht mit einer dieser Signaturfreigabemethoden registriert wurde, ist für die Nutzung der Teilnehmerapplikation eine Neuregistrierung notwendig.		P
13.	Freischaltung der Kommunikationskanäle für das konfigurierte Zugangszertifikat, welches auf dem CSR basiert	P	
14.	Ggfs. Konfiguration der Firewall, serverseitig beim Teilnehmer.		P

Tätigkeiten (S = STS/T = Teilnehmer)	S	T
15. Benennung eines Verantwortlichen inklusive laufender Stellvertretung für alle Fragen bezüglich der Technik, Sicherheit und Durchführung der Registrierung von Signierenden und Ansprechpartner für Auditfragen.		P
16. Aufschalten des Teilnehmers und Zusenden der teilnehmerspezifischen Zugangsdaten.	P	
17. Einbindung des Signing Service in die teilnehmerspezifische Anwendung(en) bzw. teilnehmerseitige Anbindung der Schnittstelle zum Signing Service und ggfs. Multiple Authentication Broker, z.B. durch Einsatz einer Partnerapplikation.		P
18. Prüfung des Zugriffs auf den Signing Service und ggfs. Multiple Authentication Server und der Ausstellung von Signaturen bzw. Siegeln oder Zeitstempeln. Umgehende Meldung allfälliger Fehler, bevor die Signaturen benutzt werden.		P
19. Fehlerbehebung durch Update oder Neuinstallation.	P	
20. Meldung der Aufgabe der Geschäftstätigkeit sowie eine gegen ihn gerichtete Konkursandrohung, die erfolgte Konkurseröffnung oder eine Nachlassstundung.		P
Beendigung des Service		
1. Löschen der Teilnehmerberechtigungen in der Signing Service Infrastruktur.	P	
2. Löschen der Schlüssel aus dem HSM.	P	

Wiederkehrende Leistungen

Tätigkeiten (**S = STS/T = Teilnehmer**)	S	T
Standardleistungen		
1. Betrieb der Signing Service und Smart Registration Service Infrastruktur.	P	
2. LifeCycle Management der Signing Service und Smart Registration Service Infrastruktur.	P	
3. LifeCycle Management der Infrastruktur des Teilnehmers: Anpassung an den aktuellen Stand der Technik und Sicherheit (Security Patches, Updates usw.).		P
4. Angemessene technische und organisatorische Massnahmen zum Schutz der von der Teilnehmerapplikation übermittelten Daten (z.B. auch durch Abschaltung nicht benötigter Zugänge, Zugangsregelungen etc.). Offenlegung des Sicherheitsdispositivs der Teilnehmerapplikation und der Kommunikation zu dem Swisscom Zertifizierungs- und/oder Vertrauensdienst, sofern von Swisscom Trust Services oder der Anerkennungsstelle von Swisscom (Schweiz) AG bzw. Swisscom ITSF verlangt.		P
5. Anpassung der Definition der Sicherheitsanforderungen.	P	
6. Lifecycle-Management des SSL/TLS-Zugangszertifikates: Option "Personensignaturen" und "Zeitstempel": rechtzeitiger Austausch bei Ablauf der Gültigkeit durch den benannten Sicherheitsverantwortlichen durch E-Mail des CSR an **sts.salessupport@swisscom.com** unter Bezeichnung des Kontonamens. Option "Siegel": rechtzeitiger Austausch vor Ablauf der Gültigkeit durch den Siegelersteller selber mittels E-Mail an den 1st Level Support der Swisscom Trust Services unter Bezeichnung der Claimed Identity.		P
7. Erstellung von Signaturzertifikaten, Siegel und Zeitstempel nach dem Standard X.509.	P	
8. Festlegung der Signatur-/Siegelzertifikatsinhalte und Verfahren zur Signatur- und Siegelerstellung.	P	
9. Option "Personensignaturen": Sicherstellung des Einsatzes von technischen Signaturfreigabemethoden und vertraglich vereinbarter Signaturfreigabemethode (z.B. Mobile ID, Mobile ID App, PWD/OTP, Passkeys, etc.). Darstellung der zugelassenen Signaturfreigabemethoden im Webview (Store).	P	
10. Option "Personensignaturen": Sicherstellung vorab, dass nur diejenigen Signierenden an der Signatur teilnehmen, die mit den entsprechenden Authentifizierungsmittel für die Signaturart registriert und zugelassen sind, sonst erfolgt (je nach Konfiguration optional) eine Weiterleitung zum Identifizierungsdienst. Darstellung der zugelassenen Identifikationsmethoden im Webview (Store).	P	
11. Option "Personensignaturen": Ansprache der registrierten Signaturfreigabemethode, sofern in der Signaturanfrage ein registrierter Hinweis auf den Signierenden (z.B. Mobilnummer, uuid, E-Mail etc.) mitgegeben wird.	P	

Tätigkeiten (**S = STS/T = Teilnehmer**)	S	T
12. Durchführen von Signaturen, für die eine Signaturfreigabe des Signierenden vorliegt.	P	
13. Signatur in Verbindung mit einem qualifizierten Zeitstempel nach ZertES und eIDAS.	P	
14. Sicherstellung der Vertraulichkeit des Datenaustauschs zwischen dem Swisscom Zertifizierungs- und/oder Vertrauensdienst und dem Teilnehmer (z.B. Vermeidung von "Inspection" Modulen zum Aufbrechen der TLS-Verbindung).		P
15. Sofern geregelte oder qualifizierte elektronische Siegel erstellt werden: Auswahl eines kryptographischen Moduls oder HSM, das den Zugriff auf die Teilnehmerapplikation spätestens nach 5 Fehlversuchen zur Authentisierung am Service sperrt. Es muss nach einer Sperrung ein neues Zugangszertifikat in einer gemeinsamen Zeremonie mit Swisscom Trust Services erstellt werden.		P
16. Option "Siegel": Übermittlung der Daten des Siegelerstellers (Distinguished Name) gemäss den Vorgaben im Zertifikatsantrag des Siegelerstellers und in der Annahmeerklärung.		P
17. Sicherstellen der Mitwirkungsleistungen und Auflagen durch den Sicherheitsverantwortlichen.		P
18. Bereitstellung der Supportdienstleistungen (Service Desk, Incident Management usw.)	P	
19. Zählung aller Signatur-, Registrierungs- und Signaturfreigabeanfragen gemäss dem Verrechnungsmodell und summarische Verrechnung an den Teilnehmer. Es findet keine Darstellung auf den einzelnen Signierenden statt. Auskünfte hierüber gibt es nur mittels anonymisierter Daten im Supportfall.	P	
20. Errichtung eines Abrechnungssystems und Zählung aller Signaturanfragen und Verrechnung mit dem Signierenden bzw. Zuordnen von Signaturfragen zu unterschiedlichen Endkunden des Teilnehmers. In die Verrechnung einbezogen werden müssen alle möglichen Verfahren von Signaturfreigaben und optionalen Identifikationen, die ein Signierender im Rahmen dieser Signatur durchführt.		P
21. Melden von Mutationen der teilnehmerspezifischen Informationen (Kontaktpersonen, SSL/TLS Zugangszertifikat usw.)		P
22. Nachführen der teilnehmerspezifischen Informationen (Kontaktpersonen, SSL/TLS Zugangszertifikat usw.)	P	
23. Melden von Sicherheitsvorfällen auf dem System der Teilnehmerapplikation, die den Signing Service oder Smart Registration Service betreffen.		P
24. Melden von Sicherheitsvorfällen auf dem System des Signatur- oder Smart Registration Service, die Auswirkung auf den Teilnehmer hat.	P	
25. Entscheid und Verantwortung für rechtliche Wirkungen der gewählten Signaturart bzw. Signaturniveau (vgl. Kapitel 8.2)		P
26. Anzeige an den Signierenden, ob es sich um eine fortgeschrittene oder qualifizierte Signatur bzw. fortgeschrittenes, qualifiziertes oder geregeltes Siegel handelt		P
27. Betrieb einer Revokationsstelle zur Ungültigkeitserklärung eines Siegelzertifikates bei Kompromittierung oder aus anderen Gründen	P	
28. Revozieren und Ermöglichung von Revokationen durch den Siegelersteller bei Anzeichen einer Kompromittierung vom Siegel- oder Zugangszertifikat über ein von Swisscom Trust Services publiziertes Revokationsverfahren.		P
29. Weiterentwicklung, Anpassung der Schnittstelle an aktuelle regulatorische und Sicherheits-Vorgaben. Information über Schnittstellenanpassung 3 Monate vor Release, sofern kein sofortiger Handlungsbedarf gesetzlich oder aus Sicherheitsgründen gegeben ist. Maximal 2 Anpassungen pro Jahr		P
30. Anpassung der Schnittstellen an die neuen Vorgaben von Swisscom Trust Services binnen drei Monaten.		P

5.2 Option: Nutzung für Signierende mit Wohnsitz ausserhalb der Schweiz, EU und EWR

Tätigkeiten (**S = STS/T = Teilnehmer**)	S	T
Leistungen bei optionaler Nutzung für Signierende mit Wohnsitz ausserhalb Schweiz, EU und EWR (nachfolgend wird das Land des Signierenden als «RoW Wohnsitzland» bezeichnet, RoW = Rest of World)		
1. Kostenpflichtige Prüfung der Einsatzmöglichkeiten für Signierende des beabsichtigten RoW Wohnsitzlandes im Hinblick auf geltenden Konsumentenschutz, Datenschutz, Kryptographie und Einsatzvorgaben sowie technischen Möglichkeiten (z.B. SMS-Empfang) unter Einbezug von Experten. Abhängig von der Einsatzprüfung ist ein Einsatz möglich mit den in den nachfolgenden Punkten	P	

Tätigkeiten (**S = STS/T = Teilnehmer**)	S	T
beschriebenen Leistungen oder ein Einsatz ist nicht möglich und der Teilnehmer wird hierüber informiert.		
2. Verzicht auf das Angebot von Signaturen für Signierende mit Wohnsitz im RoW Wohnsitzland, sofern die Einsatzprüfung unter Punkt 1. ergeben hat, dass ein Einsatz nicht in diesem Wohnsitzland möglich ist.		P
3. Bei positiver Einsatzprüfung: Erfüllung der rechtlichen Auflagen: • Anpassung der Nutzungsbestimmungen im Hinblick Konsumenten- und Datenschutz • Erfüllung der Datenschutzauflagen des Wohnsitzlandes (z.B. Pflege eines speziellen Datenverarbeitungsverzeichnisses, Stellen eines Datenschutzbeauftragten, etc.) • Konfiguration im Hinblick auf erlaubte Krypto Algorithmen • Erfüllung der Auflagen für den Einsatz der Signaturfreigabemethode im Wohnsitzland (z.B. Voranmeldung von SMS-Absendernummern, Google Play oder Apple Store Bedingungen, etc.)	P	
4. Akzeptanz, dass Registrierungen des Signierenden in seinem RoW Wohnsitzland ohne Angemessenheitsbeschluss des Bundesrates nach geplantem Datenschutzgesetz Art. 16 der Schweiz bzw. der Europäischen Kommission nach Art. 45 Abs. 3 DSGVO aufgrund der erhöhten Datenschutzanforderungen nicht erfolgen können (z.B. kein Einsatz der RA-App) sondern nur Fernregistrierungen möglich sind (z.B. Videoidentifikation), sofern zugelassen.		P
5. Akzeptanz, dass der Zertifizierungs- oder Vertrauensdienst seine Haftung auf 5'000 CHF pro Signatur im Zertifikat (QES/FES) begrenzen kann. Der Teilnehmer hat den Signierenden hierauf hinzuweisen.		P
6. Akzeptanz von Auflagen für den Einsatz im Wohnsitzland: • Z.B. Einschränkung des zu verwendenden Signaturfreigabemethode (z.B. alleinige Nutzung von Mobile ID App oder alleinige Nutzung eines kundenspezifischen Verfahrens) • Z.B. Einschränkungen im Hinblick auf die einzusetzenden Identifikationsmethoden		P
7. Erstellung einer sprachlich angepassten Version der Nutzungsbestimmungen oder anderen regulatorischen Texten für das RoW Wohnsitzland, sofern notwendig,	P	
8. Technisch und organisatorische Anpassungen, wie z.B. • Erweiterung und Abklärung der Registrierung mit den Registrierungspartnern des Smart Registration Service oder anderen Registrierungspartnern oder Authentifizierungspartner • Auswahl von geeigneten SMS-Provider, Anpassungen von SMS-Texten (z.B. Unicodevorgaben) • Einstellen einer app-basierten Signaturfreigabemethode im Google Play Store oder Apple Store • Information an den Auditor bzw. Zulassungsstelle • Einstellung der Limite für die Haftung im Zertifikat und in den Nutzungsbestimmungen, Bindung der registrierten Signierenden ausschliesslich an den Zugang der Teilnehmerapplikation dieses Vertrages	P	
9. Akzeptanz, dass nicht alle Signaturfreigabemethoden im jeweiligen Zielland unterstützt werden können (z.B. Akzeptanz von SMS wird unterdrückt).		P
10. Laufende Beobachtung der rechtlichen Regelungen (Änderungen im Konsumentenrecht, Datenschutzrecht, etc.) und technischen Voraussetzungen im RoW Wohnsitzland, die Auswirkungen auf Signierende mit Wohnsitz in diesem Land haben können. Information des Teilnehmers über diese Änderungen. Erstellung eines Angebotes für notwendige Änderungen zur Fortführung des Signaturangebotes oder Information an den Teilnehmer über das notwendige Einstellen des Signaturangebotes im RoW Wohnsitzland (sofern möglich, 3 Monate vor Inkrafttreten)	P	
11. Im Falle von notwendigen Anpassungen gemäss Ziffer 8, Beauftragung der notwendigen Änderungen oder Einstellung des Signaturservices für Signierende dieses RoW Wohnsitzlandes gemäss Fristsetzung.		P

6 Service Level und -Reporting

6.1 Service Level

Die nachfolgenden Service Levels beziehen sich grundsätzlich auf die vereinbarte Monitored Operation Time. Definitionen der Begriffe (Operation Time, Monitored Operation Time, Support Time, Availability, Security und Continuity) sowie die Beschreibung des Messverfahrens und des Reportings ergeben sich aus dem Vertragsbestandteil „Basisdokument". Folgende Service Levels werden für die Serviceausprägungen (siehe Kapitel 4) erbracht. Bei mehreren möglichen Service Levels pro Ausprägung erfolgt die Auswahl des Service Levels im Servicevertrag.

Service Level & Zielwerte			Smart Registration & Signing Service
Operation Time			
Monitored Operation Time	Mo-So 00:00-24:00		
Provider Maintenance Window	PMW-DC	PMW Data Center Swisscom (Schweiz) AG	●
	PMW-S mit Vorankündigung für sicherheits- und systemkritische Updates	Täglich 19:00-07:00, nur für angekündigte Wartungen	●
Support Time			
Support Time[1]	Mo-Fr 08:00-17:00[2]		●
Störungsannahme	Mo-So 00:00-24:00		●
Availability			
Service Availability			
Signaturservice	99.8%		●
Verzeichnisdienste nach CP/CPS Ziffer 2.1	99.9%		●
Security			
	Siehe Basisdokument		●
Continuity			
Service Continuity (STSSC)[3]	RTO 4 h | RPO 1 h		●

● = Standard (im Preis inbegriffen) ○ = Gegen Aufpreis — = Nicht erhältlich

6.2 Service Level Reporting

Auf besondere Anfrage kann ein Service Level Report über die Availability des betreffenden Monats erstellt und dem Teilnehmer übergeben werden.

7 Rechnungsstellung und Mengenreport

7.1 Rechnungsstellung

Die Details zur Rechnungsstellung werden im Service Vertrag bzw. der AGB geregelt.
Grundsätzlich gibt es folgende Verrechnungsverfahren:

[1] Wurde der Signing Service über einen Swisscom Partner bezogen so ist dieser grundsätzlich bei Störungen zu kontaktieren. Der Partner wird die Störung an Swisscom weiterleiten, sofern er diese nicht beheben kann.
[2] Feiertagsregelung siehe "Basisdokument (Kapitel SLA-Definitionen)"
[3] RTO und RPO beziehen sich nur auf die Bereitstellung des Signing Service Service am SAIP. Mobilfunkdienste, die für die Identifikation, Authentifikation oder Willensbekundung genutzt werden, sind hier nicht erfasst.

7.1.1 Vergütung nach Abruf - Postpaid Modell

Hierbei werden im Nachgang die abgerufenen Mengen von signierten oder gesiegelten Dokumentenhashes des letzten Leistungszeitraumes gezählt und mit dem für diese Bezugsmenge vorgesehenen Preis im Servicevertrag verrechnet. Bei einer Stapelsignatur wird jeder enthaltene Hash einzeln verrechnet.

7.1.2 Vergütung nach volumengebundenen Nutzungspreismodell – Prepaid Modell für Personensignaturen

Hierbei bestimmt der Teilnehmer sowohl den geplanten Leistungszeitraum als auch die geplante Anzahl der Signaturen vorab. Er verpflichtet sich zu dieser Mengenabnahme während des Leistungszeitraumes und zahlt hier im Vorhinein einen vertraglich vereinbarten Preis, der über die Zeitdauer hinweg in regelmässigen Raten gemäss Servicevertrag entrichtet wird. Darüberhinausgehende Volumina werden wie in 7.1.1. beschrieben im Nachgang gemäss Preis im Servicevertrag verrechnet. Eine Erhöhung oder Verringerung des Volumens bzw. der Vertragslaufzeit ist unter gewissen Umständen während der Vertragslaufzeit durch Abschluss eines Neuvertrages und ggfs. Deltazahlungen möglich. Signaturen werden in Leistungseinheiten umgerechnet, so dass die eingekauften Leistungseinheiten für verschiedene Produkte (z.B. fortgeschrittene und qualifizierte Zertifikate oder EU/Schweiz) verwendet werden können.

7.1.3 Paketvergütungen

Es können Pakete angeboten werden, die ein bestimmtes Volumen von Signaturen beinhalten inklusive der hierfür notwendigen Registrierungen und Signaturfreigaben. Hierbei wird eine monatliche oder jährliche Flatgebühr verrechnet.

7.1.4 Vergütung von Signaturfreigaben und Registrierungen

Diese werden in einer eigenen Leistungsbeschreibung beschrieben.

7.2 Mengenreport

In den Abrechnungen werden bei den Vergütungen nach Abruf die Summen der Hashes des betreffenden Leistungszeitraums angegeben. Anonymisierte Reports mit allen Signaturabfragen zu einem Leistungsmonat können auf Bedarf zur Klärung von Problemen angefragt werden. Swisscom Trust Services behält sich vor, bei regelmässigen Anfragen die Lieferung der Einzelleistungsreports in Rechnung zu stellen. Es werden keine nutzerspezifischen Abrechnungen erstellt. Rechnungen werden pro Zugang (sogenannte «UUID» oder «ClaimedID») erstellt.

8 Besondere Regelungen

8.1 Teilnehmerapplikation

Die Teilnehmerapplikation und ein Abrechnungsmodul für den einzelnen Signierenden ist nicht Bestandteil dieser Leistungsbeschreibung. Sie werden durch den Teilnehmer selbst, durch einen Swisscom Trust Services Partner oder Swisscom Trust Services selber beigestellt.

8.2 Signaturarten der Personensignatur und deren Einsatzmöglichkeiten

Es obliegt dem Teilnehmer, die Rechtswirkungen der gewählten Art der elektronischen Signatur (mit und ohne Zeitstempel), die den Signierenden verfügbar gemacht wird, im Voraus fachmännisch abzuklären. Swisscom Trust Services übernimmt hierfür keine Verantwortung:

Qualifizierte elektronische Signatur der Schweiz nach ZertES (QES, Zertifikat der Swisscom (Schweiz) AG - Klasse Diamant): Die über den Signing Service erstellte QES erfüllt die in der CP / CPS definierten Eigenschaften und die Definition gemäss Art. 2 Bst. e des Schweizer Bundesgesetzes über die elektronische Signatur (ZertES; SR 943.03). Nur die mit einem qualifizierten Zeitstempel verbundene QES ist bei Anwendung von Schweizer Recht der eigenhändigen Unterschrift gleichgestellt, sofern keine abweichenden gesetzlichen oder vertraglichen Regelungen vorgehen (Art. 14 Abs. 2bis Schweizer Obligationenrecht).

Qualifizierter elektronischer Zeitstempel: Der über den Signing Service erstellte qualifizierte elektronische Zeitstempel erfüllt die in der CP / CPS definierten Eigenschaften und die Definition gemäss Art. 2 Bst. j ZertES und die Definition gemäss Art. 3 Ziff. 34 eIDAS-VO mit den Rechtswirkungen gemäss Art. 42 eIDAS-VO.

Fortgeschrittene elektronische Signatur der Schweiz (FES, Zertifikat der Swisscom (Schweiz) AG -Klasse Saphir): Die über den Signing Service erstellte FES erfüllt die in der CP / CPS definierten Eigenschaften. Die FES ist (im Unterschied zur QES) in der Schweiz nicht gesetzlich geregelt und genügt nicht dem rechtlichen Erfordernis der Schriftlichkeit im Sinne des Artikels 12 des Schweizer Obligationenrechts, sie hat also nicht die gleichen Rechtswirkungen wie eine handschriftliche Unterschrift. Das rechtliche Erfordernis der handschriftlichen Unterschrift (Formvorschrift der einfachen Schriftlichkeit) kann elektronisch grundsätzlich nur durch die mit einem qualifizierten elektronischen Zeitstempel verbundene QES gleichwertig ersetzt werden, die nicht mit der FES auf der Basis von fortgeschrittenen Zertifikaten zu verwechseln ist.

Qualifizierte elektronische Signatur der EU nach eIDAS-VO (QES, Zertifikat der Swisscom ITSF-Klasse Diamant): Die über den Signing Service erstellte QES erfüllt die in der CP / CPS definierten Eigenschaften und die Definition gemäss Art. 3 Ziff. 12 eIDAS-VO mit den Rechtswirkungen gemäss Art. 25 eIDAS-VO.

Fortgeschrittene elektronische Signatur der EU nach eIDAS-VO (FES, Zertifikat der Swisscom ITSF -Klasse Saphir): Die über den Signing Service erstellte FES erfüllt die in der CP / CPS definierten Eigenschaften und die Definition gemäss Art. 3 eIDAS-VO mit der Rechtwirkung gemäss Art. 25 Abs. 1 eIDAS-VO. Die FES hat nicht die gleichen Rechtswirkungen wie eine handschriftliche Unterschrift oder eine QES.
Je nach Situation benötigen gewisse Dokumente also die handschriftliche Unterschrift oder die QES und in der Schweiz verbunden mit einem qualifizierten elektronischen Zeitstempel, damit beabsichtigte Rechtswirkungen überhaupt eintreten können.
Über Signing Service erstellte elektronische Signaturen gemäss den Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten ausgestellt von den Issuing CAs "Diamant“ (qualifiziert) und „Saphir“ (fortgeschritten) können bei Anwendbarkeit ausländischen Rechts abweichende, allenfalls weitergehende oder weniger weitgehende Wirkungen entfalten als dies nach Schweizer Recht oder nach Recht der EU der Fall ist.
Der Austausch verschlüsselter Daten und die Ausstellung von Zertifikaten unterliegt zudem in/mit gewissen Staaten gesetzlichen Restriktionen.

8.3 Einsatzmöglichkeiten des fortgeschrittenen oder geregelten elektronischen Siegels

Die Verwendung des fortgeschrittenen oder geregelten elektronischen Siegels dient in der Regel dazu, den Herkunftsnachweis sowie die Integrität des Inhalts einer Datei zu gewährleisten. Das elektronische Siegel ist nicht mit dem rechtlichen Konzept der elektronischen Signatur zu verwechseln. Zudem sind die Rechtswirkungen des höherwertigen geregelten elektronischen Siegels nicht dieselben wie diejenigen des fortgeschrittenen elektronischen Siegels. Es obliegt dem Teilnehmer und seinen Siegelersteller, die Rechtswirkungen der gewählten Art der elektronischen Siegel (mit und ohne Zeitstempel) im Voraus abzuklären. Swisscom Trust Services übernimmt hierfür keine Verantwortung.
Geregeltes elektronisches Siegel nach Schweizer ZertES (auf der Basis eines Zertifikats der Swisscom (Schweiz) AG-Klasse Diamant): Das über den Signing Service erstellte geregelte Siegel erfüllt die in der CP/CPS definierten Eigenschaften und die Definition gemäss Art. 2 Bst. d des Schweizer Bundesgesetzes über die elektronische Signatur (ZertES; SR 943.03).
Fortgeschrittenes elektronisches Siegel für die Schweiz (Zertifikat der Swisscom (Schweiz) AG-Klasse Saphir): Das über den Signing Service erstellte fortgeschrittene elektronische Siegel erfüllt die in der CP/CPS definierten Eigenschaften und ist im Unterschied zum geregelten elektronischen Siegel nicht gesetzlich geregelt.
Qualifizierter elektronischer Zeitstempel: Der über den Signing Service erstellte qualifizierte elektronische Zeitstempel erfüllt die in der CP / CPS definierten Eigenschaften und die Definition gemäss Art. 2 Bst. j ZertES und die Definition gemäss Art. 3 Ziff. 34 eIDAS-VO mit den Rechtswirkungen gemäss Art. 42 eIDAS-VO.
Qualifizierte elektronische Siegel nach eIDAS-VO (EU) (Zertifikat der Swisscom ITSF-Klasse Diamant): Das über den Signing Service erstellte qualifizierte elektronische Siegel erfüllt die in der CP/CPS definierten Eigenschaften und die Definition gemäss Art. 3 Ziff. 27 eIDAS-VO mit den Rechtswirkungen gemäss Art. 35 eIDAS-VO.
Fortgeschrittenes elektronisches Siegel nach eIDAS-VO (EU) (Zertifikat der Swisscom ITSF-Klasse Saphir): Das über den Signing Service erstellte fortgeschrittene elektronische Siegel erfüllt die in der CP/CPS definierten Eigenschaften und die Definition gemäss Art. 3 Ziff. 26 eIDAS-VO mit der Rechtswirkung gemäss Art. 35 eIDAS-VO.
Weder das fortgeschrittene elektronische Siegel noch das geregelte elektronische Siegel haben die gleichen Rechtswirkungen wie eine handschriftliche Unterschrift oder eine qualifizierte elektronische Signatur. Je nach Situation benötigen gewisse Dokumente also die handschriftliche Unterschrift, eine qualifizierte elektronische Signatur oder ein geregeltes elektronisches Siegel ggfs. mit einem elektronischen Zeitstempel, damit beabsichtigte Rechtswirkungen überhaupt eintreten können.
Über den Signing Service ausgestellte elektronische Siegel können bei Anwendbarkeit ausländischen Rechts abweichende, allenfalls weitergehende oder weniger weitgehende Wirkungen entfalten als dies nach Schweizer Recht oder Recht der EU der Fall ist.
Der Austausch verschlüsselter Daten und die Ausstellung von Zertifikaten unterliegt zudem in/mit gewissen Staaten gesetzlichen Restriktionen.

8.4 Betrieb der Teilnehmerapplikation, wenn Teilnehmer und Siegelersteller nicht identisch sind

Die im Zertifikatsantrag befugte Vertreterin des Siegelerstellers muss das Zugangszertifikat Swisscom Trust Services übergeben oder bei fortgeschrittenen Siegeln der Übergabe des Zugangszertifikates an Swisscom Trust Services durch den Teilnehmer schriftlich zustimmen. Dadurch wird der Teilnehmer zum Betrieb der Teilnehmerapplikation für den Siegelersteller gegenüber dem Swisscom Zertifizierungs- bzw. Vertrauensdienst autorisiert. Sofern die befugte Vertreterin wechselt, ist das Swisscom Trust Services schriftlich oder per E-Mail durch einen Vertreter des Siegelerstellers oder durch die bisherige Kontaktperson anzuzeigen.
Insofern werden alle über die Schnittstelle zum Swisscom Zertifizierungs- oder Vertrauensdienst übertragenen Dokumente mit einem elektronischen Siegel versehen. Die Swisscom Systeme können nicht überprüfen, ob der Zugriff des Betreibers der Teilnehmerapplikation mit Zugriffsvollmacht auf das Schlüsselmaterial zum Siegelerstellen berechtigt war oder irrtumsfrei erfolgt ist.

8.5 Datenbearbeitung durch Dritte aus dem In- oder Ausland, Notfallzugriffe

Die im Rahmen der Leistungserbringung vom Teilnehmer an den Swisscom Zertifizierungs- oder Vertrauensdienst im Auftrag des Signierenden übermittelten Signaturanfragen (Teilnehmerdaten) werden grundsätzlich durch Swisscom (Schweiz) AG - auch für die Swisscom IT Services Finance S.E. - in der Schweiz bearbeitet. Eine Datenbearbeitung durch beigezogene Dritte und/oder aus dem Ausland erfolgt ausschliesslich im Einklang mit den einschlägigen Vorschriften der schweizerischen Datenschutzgesetzgebung. Solche Bearbeitungen können insbesondere durch Mitarbeitende mit Wohnsitz in der EU (Grenzgänger) oder auf Reisen sowie durch Wartungsabteilungen von Herstellerfirmen aus der EU stattfinden. Im Rahmen des vorliegenden Service sind namentlich folgende Konstellationen von einer solchen Bearbeitung betroffen:

- Swisscom Trust Services AG bietet als Dienstleister Rollen im Rahmen Operation und Support an die Swisscom (Schweiz) AG und bearbeitet somit auch Registrierungs- und Signaturdaten unter Kontrolle und im Auftrag der Swisscom (Schweiz) AG – auch für Swisscom ITSF.
- Swisscom IT Services Finance S.E. bearbeitet via Swisscom (Schweiz) AG diejenigen Daten, die erforderlich sind, um ihren Vertrauensdienst erbringen zu können, insbesondere für die Ausstellung der elektronischen Zertifikate.
- Der 3rd Level Support des Applikationsherstellers hat in Supportfällen aus der EU temporären VPN-Zugriff auf Applikationsdaten beim Swisscom Zertifizierungs- und/oder Vertrauensdienst die ausser den vom Signierenden im Zertifikat veröffentlichten Daten keine Personendaten beinhalten. Dabei können in Einzelfällen auch die vom Signierenden im Zertifikat veröffentlichten Signaturdaten und Stammdaten der Teilnehmerorganisation (z.B. Organisationsname, Bezeichnung des vom Teilnehmer veröffentlichten TLS/SSL Zugangszertifikates) für diese Dritte ersichtlich sein. Der Zugriff wird von einem Techniker der Swisscom (Schweiz) AG oder der Swisscom Trust Services in Echtzeit überwacht, damit kein unkontrollierter Datenzugriff stattfindet und die Verbindung im Missbrauchsfall umgehend getrennt werden kann. Dieses Vorgehen entspricht den best practice Ansätzen auch für die Banken- und Versicherungsbranche.
- Aufsichtsbehörden und Konformitätsbewertungsstellen aus der Schweiz und der EU, welche die Konformität der Signaturanwendung bestätigen müssen, können im Rahmen von Audits unter Aufsicht von Swisscom (Schweiz) AG und/oder Swisscom ITSF mit Personen- und Identifikationsdaten in Kontakt kommen, um die konforme Durchführung von Identitätsprüfungen und Signaturausstellungen prüfen zu können. Diese Konformitätsprüfungen finden ausschliesslich in der Schweiz statt.

.