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

Leistungsbeschreibung
Smart Registration & Signing Service
inkl. Docusign Connector

Swisscom Trust Services

Swisscom Trust Services AG

Konradstrasse 12
8005 Zürich

Schweiz

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

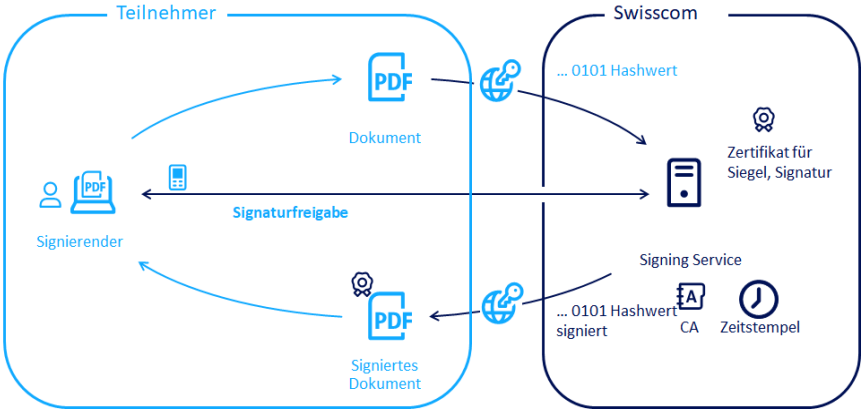
1 Inhalt

1 Inhalt 2
2 Übersicht zum Service 3
3 Definitionen 4
3.1 Service Access Interface Point (SAIP) 4
3.2 Servicespezifische Definitionen 4
4 Ausprägungen und Optionen 9
4.1 Definition der Leistungen 9
4.2 Zertifikatsinhalte 12
4.2.1 Personensignaturen 12
4.3 Ablauf der Signaturerstellung für alle Optionen in Docusign 12
4.4 Prozess zur Prüfung einer Teilnehmerapplikation 15
4.5 Datenablage und Verantwortlichkeiten 15
5 Leistungsdarstellung und Verantwortlichkeiten 16
5.1 Signaturservice 16
5.2 Option: Nutzung für Signierende mit Wohnsitz ausserhalb der Schweiz, EU und EWR 17
6 Service Level und -Reporting 19
6.1 Service Level 19
6.2 Service Level Reporting 19
7 Rechnungsstellung und Mengenreport 19
7.1 Rechnungsstellung 19
7.1.1 Vergütung nach Abruf - Postpaid Modell 20
7.1.2 Vergütung von Signaturfreigaben und Registrierungen 20
7.2 Mengenreport 20
8 Besondere Regelungen 20
8.1 Teilnehmerapplikation 20
8.2 Signaturarten der Personensignatur und deren Einsatzmöglichkeiten 20
8.3 Datenbearbeitung durch Dritte aus dem In- oder Ausland, Notfallzugriffe 21

Swisscom Trust Services

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 wie Docusign Signaturplattform 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, wie Docusign, 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. Swisscom bietet mit dem Docusign Connector ein spezielles Modul an, dass die Standard Schnittstelle von Docusign für Trust Service Provider an die Fernsignatur von Swisscom Trust Services anschliesst und die Hashübertragung und Einbettung des Hashes damit sicherstellt.

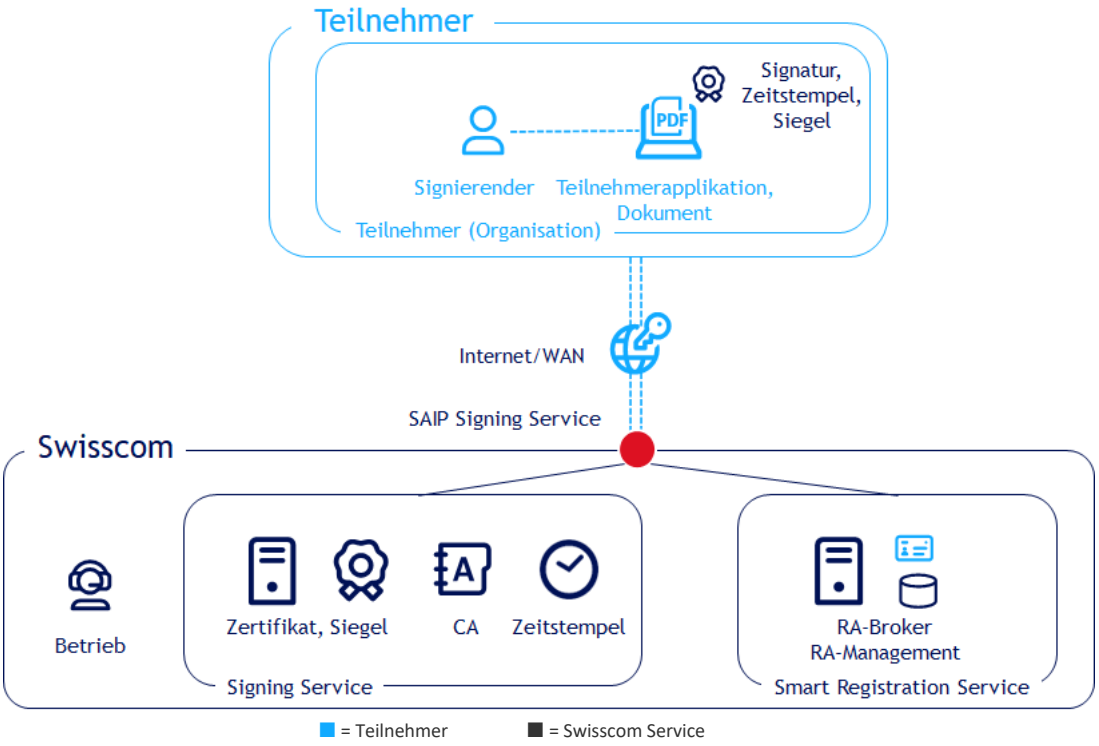


Des Weiteren bietet der Service eine einmalige, zeitlich begrenzte Registrierung und die fortwährende Nutzung eines Signaturfreigabemittels (z.B. Fingerprint App) für die Personensignatur ("Repetitive Signing"). Für die Nutzung von Identifikations- und Signaturfreigabemethode steht ein Registrierungsportal zur Verfügung, in denen Partner Ihre Identitätsprüfmethoden zur Registrierung anbieten.. Die verfügbaren Methoden sind in der " Leistungsbeschreibung Registrierungs- und Signaturfreigabemethoden" beschrieben. Darüber hinaus kann auch eine face2face Identifikation mittels RA-App oder in einem Swisscom Shop der Schweiz erfolgen.
Allgemein bietet der Signing Service je nach konkreter Vertragsgestaltung fortgeschrittene und qualifizierte elektronische Signaturen für natürliche Personen in den Rechträumen de eIDAS Verordnung (EU/EWR) und ZertES (Schweiz)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 speziell den Service für elektronische Signaturen für natürliche Personen wohnhaft in der EU, der Schweiz und EWR Staaten in Verbindung mit einem Docusign Connector.

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 – hier Docusign) 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 über die Docusign Schnittstelle https://developers.docusign.com/docs/tsp-api/tsp101/
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.
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.
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.

Begriff	Beschreibung
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.
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
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.
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.

Begriff	Beschreibung
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.
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..
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.
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.
Personensignatur	Signaturen durch natürliche Personen im Gegensatz zu Siegeln.
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

Begriff	Beschreibung
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.
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	Zertifikat, welches auf den Signierenden ausgestellt ist, von den Swisscom Zertifizierungs- und Vertrauensdiensten treuhänderisch verwaltet wird und zur Signatur bzw. Siegelerstellung verwendet wird.
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.
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.
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.

Begriff	Beschreibung
SSL/TLS	Secure Socket Layer, Transport Layer Security, Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet basierend auf SSL (Zugangs-) Zertifikaten
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.
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.
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.

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)	✓
Personensignatur: Qualifizierte elektronische Signatur eIDAS (EU)	✓
Personensignatur: Fortgeschrittene elektronische Signatur eIDAS (EU)	✓
Registrierungen in ausgewählten Swisscom Shops	✓
Registrierungen mit der RA-App	✓
Zugang zum Portal Fernregistrierungsmethoden	✓
Identifikationen und Freigaben mittels der Methoden im Store	-
Signaturfreigabe mittels Passwort und Einmalcode oder Mobile ID (App)	✓
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 - nicht unterstützt

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 und 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.
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, sofern nicht anders angegeben, ein qualifizierter elektronischer Zeitstempel immer inbegriffen.
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.
Registrierungen in ausgewählten Swisscom Shops	In ausgewählten Swisscom Shops (siehe Übersicht auf https://srsident.trustservices.swisscom.com) der Schweiz kann sich ein

Leistung	Definition
	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.
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.
Zugang zum Portal Fernregistrierungsmethoden	Swisscom Trust Services bietet über sein Registrierungsportal https://srsident.trustservices.swisscom.com/ verschiedene remote Identifikationsmethoden an. Die Registrierungen werden als Fernregistrierung durch Partner angeboten. Im Rahmen der Registrierung muss ein Signaturfreigabemittel gewählt und initialisiert werden, mit dem zukünftig Signaturen freigegeben werden.
Identifikationen und Freigaben mittels der Methoden im Store	Der Connector für Docusign ist derzeit noch nicht am Multiple Authentication Broker und den damit verbundenen erweiterten Methoden zur Fernidentifikation und weiteren Methoden zur Signaturfreigabe angebunden. Die Umsetzung ist in Planung aber dadurch stehen nur Identifikationsmethoden zur Verfügung, die in der Leistungsbeschreibung der Registrierungsmethoden mit "Portal" gekennzeichnet sind. "Store" Methoden sind hiervon ausgeschlossen.
Signaturfreigabe mittels Password und Einmalcode oder Mobile ID (App)	Nach der einmaligen Registrierung können in der Teilnehmerapplikation alle Signaturen durch folgende Signaturfreigabemethoden freigegeben werden: • Passwort / Einmalcode via SMS (PWD/OTP) Es wird ein Popup Fenster bei jedem Signaturvorgang gezeigt, bei dem ein Passwort und im nächsten Schritt ein Einmalcode eingegeben wird. Das Passwort wurde anfänglich einmalig bei der Registrierung festgelegt und darf nicht vergessen werden. Sofern das Passwort vergessen wurde, ist eine Neuregistrierung erforderlich. Der Einmalcode wird bei jedem Signaturvorgang via SMS übertragen. • Mobile ID (Schweiz) Alle SIM Anbieter / Mobilfunkanbieter der Schweiz unterstützen den Mobilfunkeigenen Service "Mobile ID", der unabhängig von den Smartphonebetriebssystemen direkt über eine App auf allen hierfür bereitgestellten SIM Karten Schweizer Anbieter funktioniert. Dieser Dienst kann einmalig über https://mobileid.ch freigeschaltet werden, ggfs. muss beachtet werden, ob Mobile ID im Tarif auch enthalten ist. Die Freigabe erfolgt dann durch einen Push der Mobile ID Funktionalität im Smartphone und der Eingabe einer PIN, die bei der Intialisierung festgelegt wurde. Während der Initialisierung wird auch ein Restaurierungscode angelegt, mit dem ein Umzug der SIM Karte auf ein neues Handy erfolgen kann. • Mobile ID App Die Mobile ID Funktionalität wird ausserhalb der Schweiz

Leistung	Definition
	insbesondere in der EU/EWR über eine entsprechende App angeboten, die im Appstore von Google Play oder Apple heruntergeladen werden kann und einmalig initialisiert werden muss. Die Freigabe kann hier sogar mittels Fingerprint oder Gesichtserkennung erfolgen, wenn das Smartphone dieses unterstützt. • Einmalcode (OTP) Qualifizierte elektronische Signaturen benötigen zur Freigabe immer zwei unabhängige Faktoren aus den Bereichen Wissen, Biometrie und Besitz (z.B. Besitz der Mobilnummer plus Fingerprintfreigabe in der App oder Besitz der Mobilnummer und Wissen der PIN). Im Falle von fortgeschrittenen elektronischen Signaturen reicht ein Faktor aus, hier kommt ein Einmalcode zu Einsatz, der per SMS an die registrierte Mobilnummer versendet wird. Da in der Schweiz alle Mobilfunkteilnehmer zur Registrierung mittels Ausweis verpflichtet sind, entfällt bei der fortgeschrittenen elektronischen Signatur mit Schweizer Mobilnummern die vorhergehende Registrierung und es kann sofort eine Bestätigung erfolgen.
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

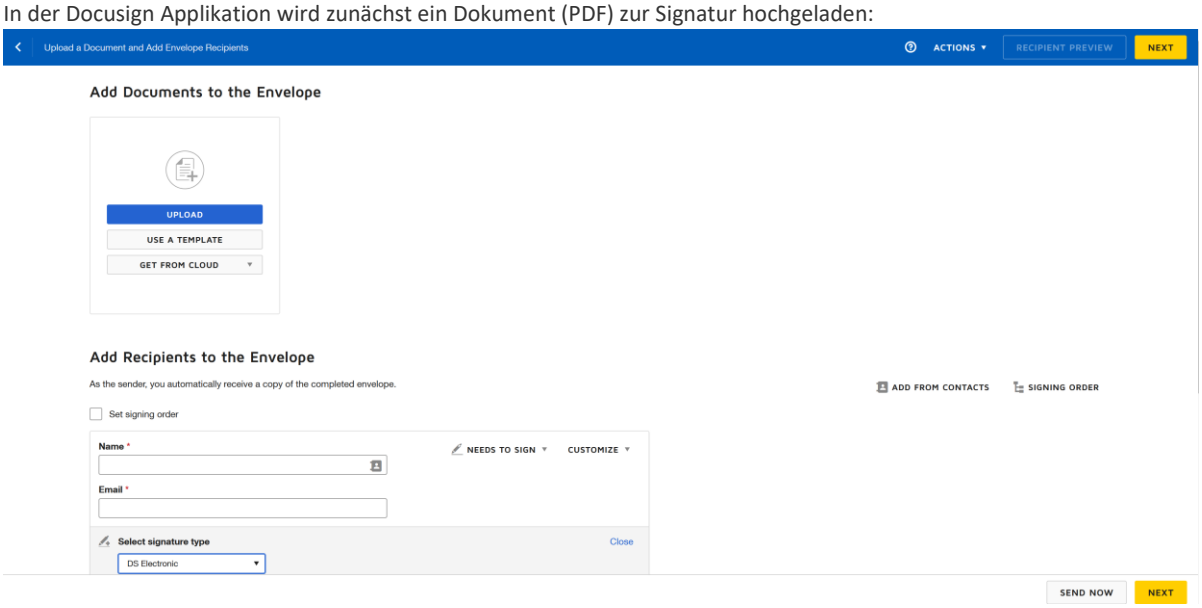
4.2.1 Personensignaturen

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 >

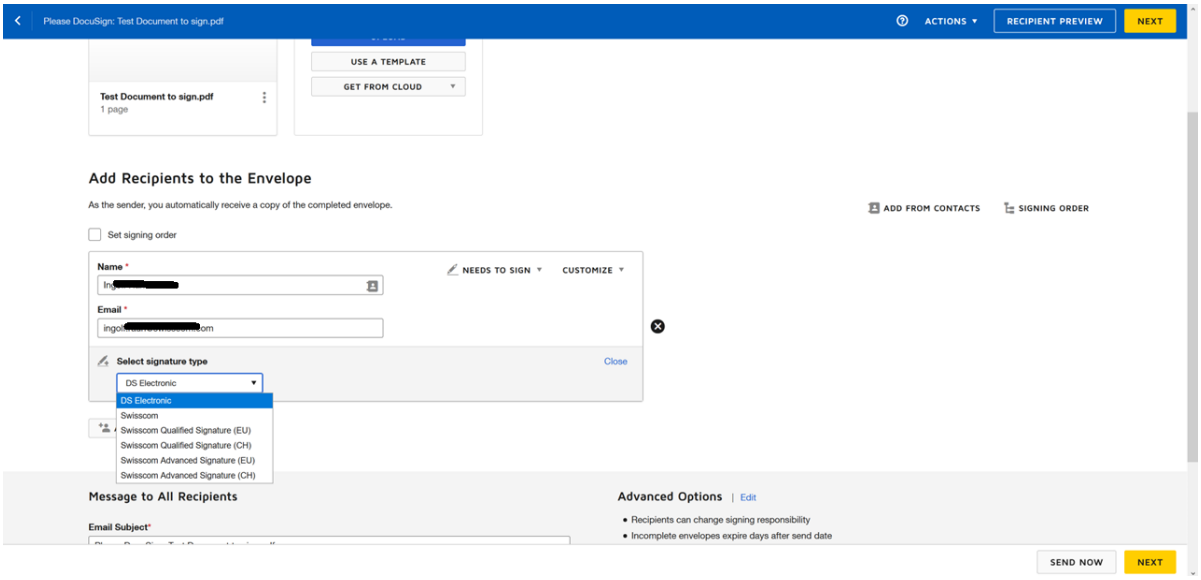
In der Leistungsbeschreibung zu den Registrierungs- und Signaturfreigabeverfahren wird das Fasttrack Verfahren beschrieben, welches die Freigabe von fortgeschrittenen elektronischen Signaturen ohne vorgängige Registrierung über eine in der Schweiz registrierte Mobilnummer erlaubt und den gesetzlichen 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">

4.3 Ablauf der Signaturerstellung für alle Optionen in Docusign

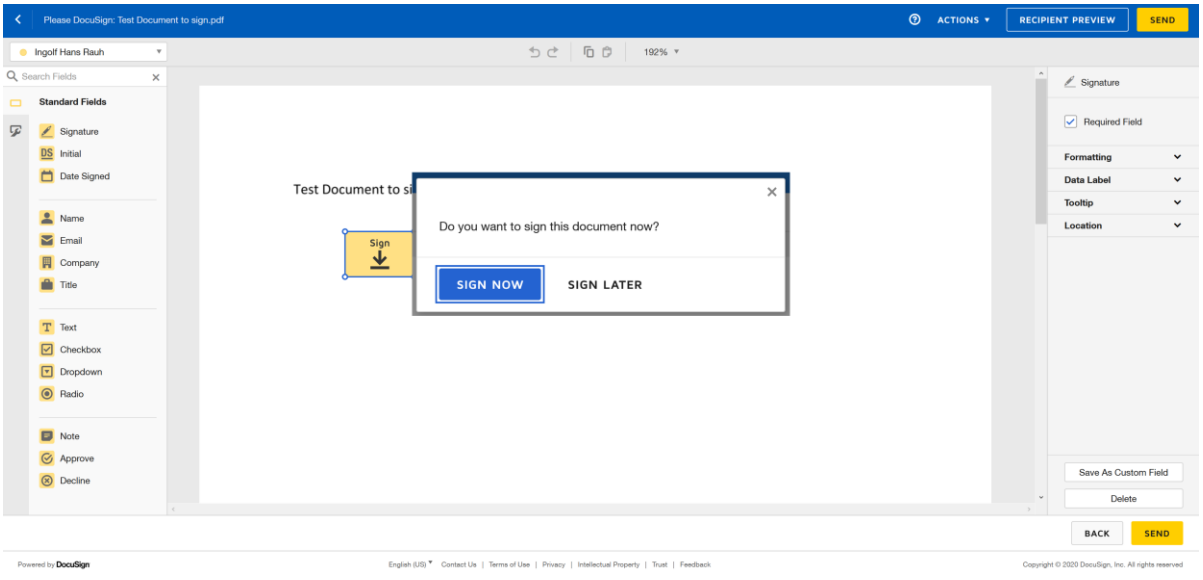
Die nachfolgenden Bilder zeichnen den typischen Ablauf der Signatur in der Teilnehmerapplikation "Docusign". Diese wird nicht von Swisscom Trust Services bereitgestellt und es kann somit zu Änderungen im Design und Ablauf kommen. Insofern dient die Ablaufbeschreibung als prinzipielle Beschreibung ohne Anspruch auf Aktualität und Richtigkeit.
In der Docusign Applikation wird zunächst ein Dokument (PDF) zur Signatur hochgeladen:



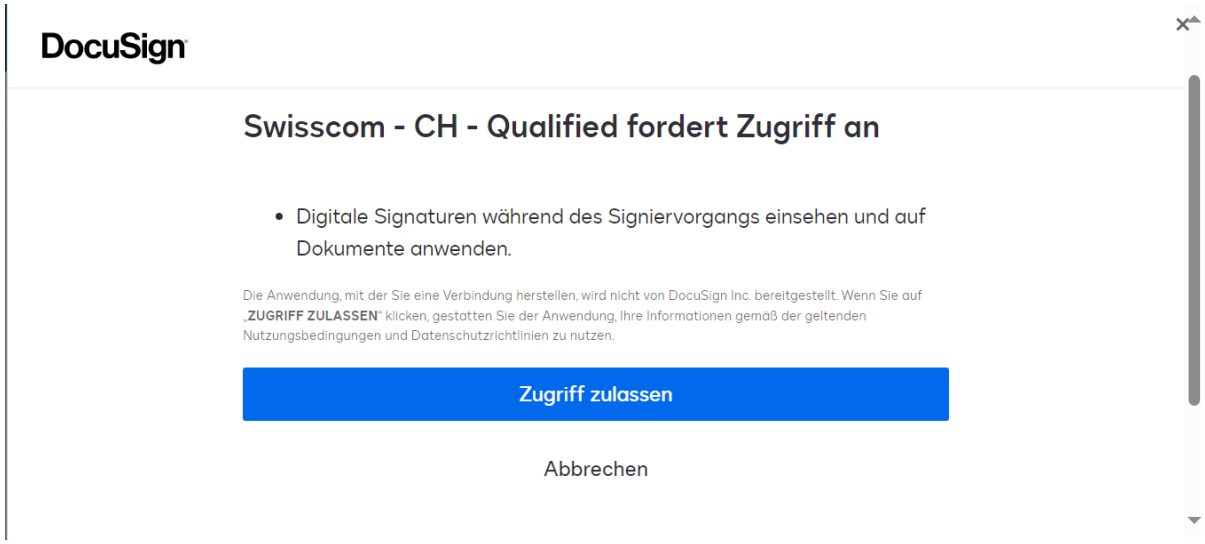
In Docusign werden nun die Unterzeichner für dieses Dokument festgelegt. Bei der Signatur muss darauf geachtet werden, den entsprechenden Signaturtyp der Swisscom Trust Services auszuwählen. Dieser beschreibt das rechtliche Anwendungsgebiet (EU/eIDAS oder Schweiz/ZertES) und die Qualität der Signatur (fortgeschritten oder qualifiziert elektronisch):



Zum Abschluss kann der Ersteller des Signaturumlaufes seine eigene Signatur setzen, sofern erwünscht, ansonsten erhalten andere Workflownutzer eine E-Mail mit einer Aufforderung zur elektronischen Signatur in ähnlicher Weise, nachdem sie den Link zum zu signierenden Dokument unterschrieben haben:



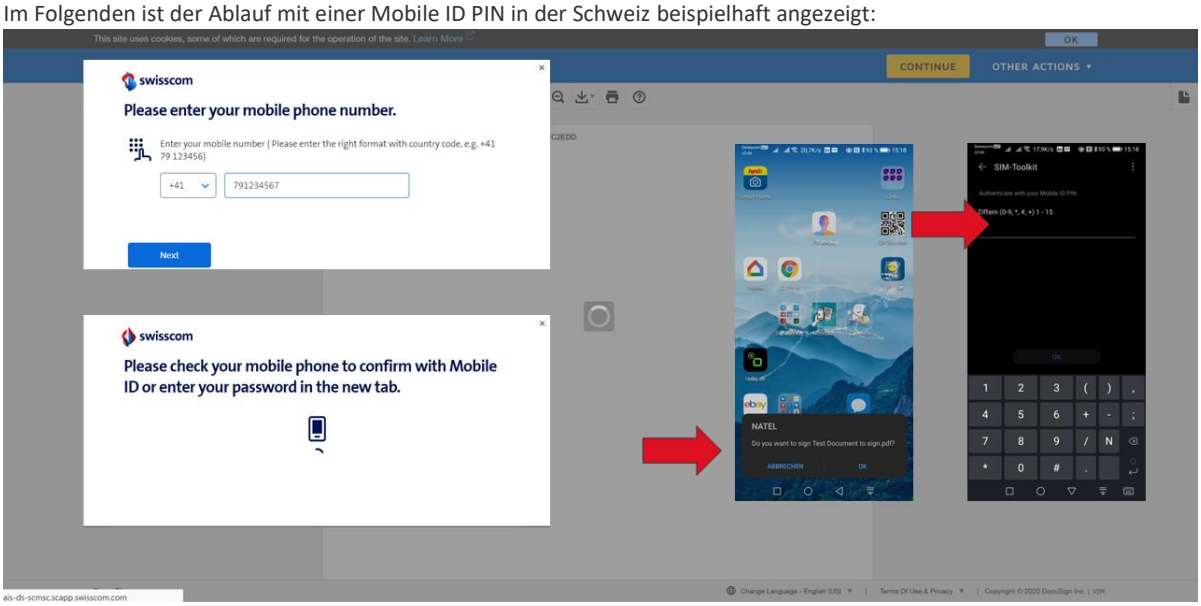
Es wird nun darauf hingewiesen, das Swisscom Trust Services in den Signaturprozess eingreift und um Zulassung des Zugriffs gebeten:



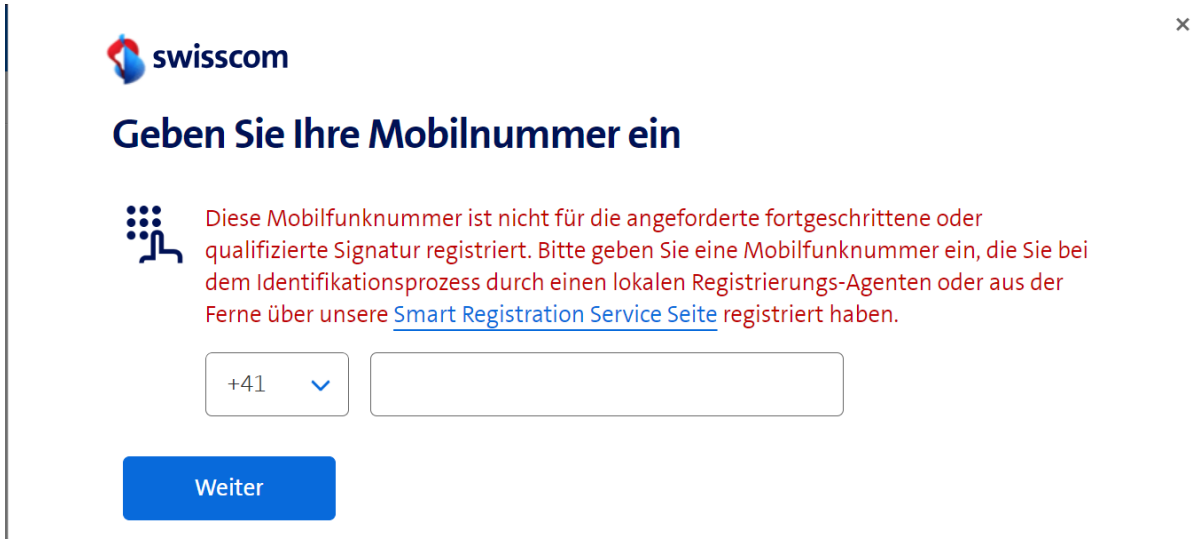
Ein registrierter Nutzer wird nun aufgefordert, seine Mobilnummer einzugeben und wird zu dem Verfahren der Signaturfreigabe weitergeleitet, welches er während der Registrierung festgelegt hat:

- Eingabe eines Passworts und Eingabe eines Einmalcodes, der via SMS empfangen wurde
- Eingabe einer Mobile ID PIN (Schweiz)
- Eingabe Fingerprint oder Gesichtserkennung in der Mobile ID App

Im Folgenden ist der Ablauf mit einer Mobile ID PIN in der Schweiz beispielhaft angezeigt:



Sollte ein Nutzer nicht registriert sein, so wird das automatisch erkannt und es wird per Link eine Weiterleitung zum Registrierungsportal für Fernidentifikationen https://srsident.trustservices.swisscom.com angeboten. Alternativ kann auch eine face2face Identifikation im Swisscom Shop der Schweiz oder mittels RA-App durchgeführt werden:



Nach der Freigabe der Signatur durch das registrierte Verfahren ist das Dokument signiert und kann binnen der Docusign Applikation heruntergeladen werden. Im Adobe PDF Reader wird ein grüner Haken angezeigt. Zusätzlich erhält das Dokument den passenden qualifizierten elektronischen Zeitstempel.

4.4 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 Verhinderung des Austauschs eines Dokumentenhash, Schutz der Applikation sichergestellt werden.

4.5 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.		✓
2. Bereitstellung der Signing Service Infrastruktur	✓	
3. Bereitstellung des Connectors zu Docusign basierend auf Docusign API für Trust Service Provider.	✓	
4. Einsatz der Teilnehmerapplikation Docusign. Konfiguration der Applikation nach den Vorgaben des Bestellsheets.		✓
5. Zusenden der unterzeichneten Annahmeerklärung mit den regulatorisch notwendigen Informationen.		✓
6. Aufschalten des Teilnehmers und Zusenden der teilnehmerspezifischen Zugangsdaten.	✓	
7. Umgehende Meldung allfälliger Fehler, bevor die Signaturen benutzt werden.		✓
8. Fehlerbehebung durch Update oder Neuinstallation.	✓	
9. Meldung der Aufgabe der Geschäftstätigkeit sowie eine gegen ihn gerichtete Konkursandrohung, die erfolgte Konkurseröffnung oder eine Nachlassstundung.		✓
Beendigung des Service		
1. Löschen der Teilnehmerberechtigungen in der Signing Service Infrastruktur.	✓	

Wiederkehrende Leistungen

Tätigkeiten (**S = STS/T = Teilnehmer**)	S	T
Standardleistungen		
1. Betrieb der Signing Service und Smart Registration Service Infrastruktur.	✓	
2. LifeCycle Management der Signing Service und Smart Registration Service Infrastruktur.	✓	
3. LifeCycle Management der Infrastruktur des Teilnehmers: Anpassung an den aktuellen Stand der Technik und Sicherheit (Security Patches, Updates usw.).		✓
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.		✓
5. Anpassung der Definition der Sicherheitsanforderungen.	✓	
6. Erstellung von Signaturzertifikaten und Zeitstempel nach dem Standard X.509.	✓	
7. Festlegung der Signaturzertifikatsinhalte und Verfahren zur Signaturerstellung.	✓	
8. Option "Personensignaturen": Sicherstellung des Einsatzes von technischen Signaturfreigabemethoden und vertraglich vereinbarter Signaturfreigabemethode (z.B. Mobile ID, Mobile ID App, PWD/OTP, etc.).	✓	
9. 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) ein Hinweis zur Weiterleitung zum Identifizierungsdienst.	✓	
10. Durchführen von Signaturen, für die eine Signaturfreigabe des Signierenden vorliegt.	✓	

Tätigkeiten (**S = STS/T = Teilnehmer**)	S	T
11. Signatur in Verbindung mit einem qualifizierten RFC3161 Zeitstempel nach ZertES und eIDAS. Ermöglichung der Teilnehmerapplikation zur Erstellung von langzeitvalidierbaren PAdES Signaturen (LTV).	✓	
12. 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).		✓
13. Bereitstellung der Supportdienstleistungen (Service Desk, Incident Management usw.)	✓	
14. 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.	✓	
15. 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.		✓
16. Melden von Mutationen der teilnehmerspezifischen Informationen (Kontaktpersonen, usw.)		✓
17. Nachführen der teilnehmerspezifischen Informationen (Kontaktpersonen, usw.)	✓	
18. Melden von Sicherheitsvorfällen auf dem System der Teilnehmerapplikation, die den Signing Service oder Smart Registration Service betreffen.		✓
19. Melden von Sicherheitsvorfällen auf dem System des Signatur- oder Smart Registration Service, die Auswirkung auf den Teilnehmer hat.	✓	
20. Entscheid und Verantwortung für rechtliche Wirkungen der gewählten Signaturart bzw. Signaturniveau (vgl. Kapitel 8.2)		✓
21. 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		✓
22. Anpassung der Schnittstellenkonfiguration an die neuen Vorgaben von Swisscom Trust Services binnen drei Monaten.		✓

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 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.		✓
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.)	✓	
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.		✓

Tätigkeiten (**S = STS/T = Teilnehmer**)	S	T
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.		✓
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		✓
7. Erstellung einer sprachlich angepassten Version der Nutzungsbestimmungen oder anderen regulatorischen Texten für das RoW Wohnsitzland, sofern notwendig,	✓	
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	✓	
9. Akzeptanz, dass nicht alle Signaturfreigabemethoden im jeweiligen Zielland unterstützt werden können (z.B. Akzeptanz von SMS wird unterdrückt).		✓
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)	✓	
11. Im Falle von notwendigen Anpassungen gemäss Ziffer 8, Beauftragung der notwendigen Änderungen oder Einstellung des Signaturservices für Signierende dieses RoW Wohnsitzlandes gemäss Fristsetzung.		✓

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.

[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.

Grundsätzlich gibt es folgendes Verrechnungsverfahren:

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 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 (Docusign) und ein Abrechnungsmodul für den einzelnen Signierenden ist nicht Bestandteil dieser Leistungsbeschreibung. Sie werden durch den Teilnehmer selbst, durch einen Swisscom Trust Services Partner, wie Docusign, 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 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.

.