



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

Leistungsbeschreibung Personensignaturen Schweiz (ZertES)

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 |
| 1 | Inhalt | 1 |
| 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 | 6 |
| 4.1 | Definition der Leistungen | 7 |
| 4.1.1 | Ablauf der Signaturerstellung für alle Optionen | 9 |
| 4.2 | Prozesse und Tools zur Personenidentifikation (Registrierungsstelle) | 10 |
| 4.2.1 | Prozess zur Organisationsprüfung | 10 |
| 4.3 | Datenablage und Verantwortlichkeiten | 10 |
| 4.4 | Willensbekundung | 11 |
| 4.5 | Option: Nutzung von DocuSign | 11 |
| 5 | Leistungsdarstellung und Verantwortlichkeiten | 11 |
| 5.1 | Signaturservice | 11 |
| 5.2 | Abrechnungsmodell «Vergütung pro aktiv Signierenden» | 14 |
| 5.3 | Option: Swisscom DocuSign Connector | 15 |
| 5.4 | Option: Eigene Identifikations- und/oder Authentisierungsmethode | 15 |
| 5.5 | Option: Nutzung für Signierende mit Wohnsitz ausserhalb der Schweiz, EU und EWR | 15 |
| 6 | Service Level und -Reporting | 17 |
| 6.1 | Service Level | 17 |
| 6.2 | Service Level Reporting | 17 |
| 7 | Rechnungsstellung und Mengenreport | 18 |
| 7.1 | Rechnungsstellung | 18 |
| 7.1.1 | Vergütung nach Abruf - Postpaid Modell | 18 |
| 7.1.2 | Vergütung pro aktiv Signierendem – Postpaid Modell | 18 |
| 7.1.3 | Vergütung nach volumengebundenen Nutzungspreismodell – Prepaid Modell | 18 |
| 7.2 | Mengenreport | 18 |
| 8 | Besondere Regelungen | 18 |
| 8.1 | Teilnehmerapplikation | 18 |
| 8.2 | Signaturarten und deren Einsatzmöglichkeiten | 18 |
| 8.3 | Datenbearbeitung durch Dritte aus dem In- oder Ausland, Notfallzugriffe | 19 |

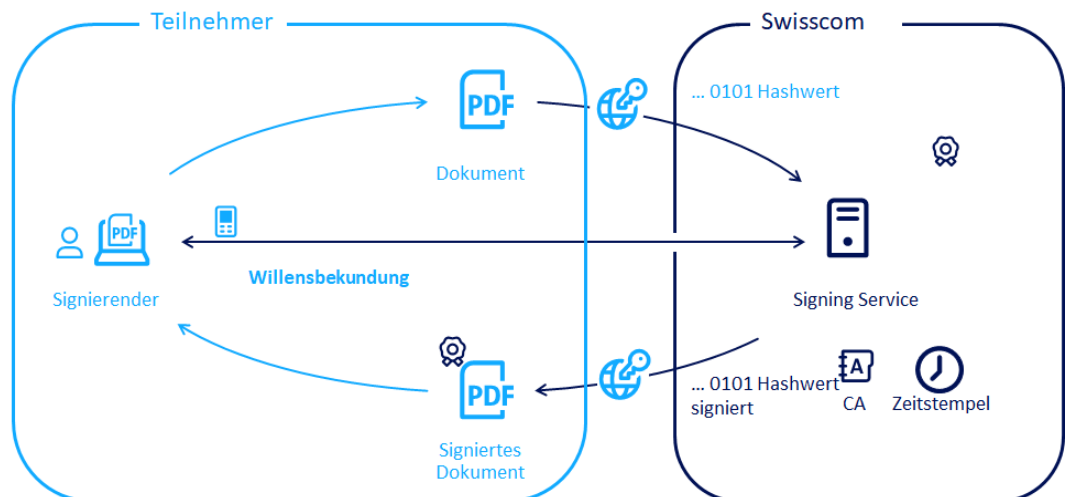


2 Übersicht zum Service

Der Signing Service ist eine serverbasierte Fernsignaturdienstleistung vertrieben durch Swisscom Trust Services AG und erbracht durch die Swisscom (Schweiz) AG in den Rechenzentren der Schweiz. Swisscom Trust Services AG vertriebt den Signing Service in eigenen Namen oder räumt Dritten wiederum das Recht ein, den Signing Service in eigenem Namen zu vertrieben.

Die Fernsignaturdienstleistung wird Teilnehmern zur Verfügung gestellt, die eine Teilnehmerapplikation betreiben. Signierende können damit digitale Dateien elektronisch signieren und sichern damit die Integrität und die Authentizität einer Datei. Swisscom (Schweiz) AG erzeugt und verwaltet für den Signierenden 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 nicht für Swisscom 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 an der Teilnehmerapplikation authentifizieren und den Willen zur Signatur bekunden. Der Signing Service nutzt hier ein zuvor registriertes Signaturfreigabemittel (z.B. Mobile ID oder ein Freigabemittel eines IDPs).



Die Identifizierung des Signierenden kann vorgängig durch nach ZertES zugelassenen Verfahren ("RA-App", "Videoidentifizierung") oder durch verschiedene auditierte Verfahren (eigene Registrierungsstelle) erfolgen.

Grundsätzlich wird bei den Signaturen zwischen fortgeschrittenen und qualifizierten elektronischen Signaturen unterschieden. 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. Eine akkreditierte Anerkennungsstelle prüft regelmässig, ob die Anforderungen, die das schweizerische Recht und / oder anerkannte technische Normen an eine Anbieterin von Zertifizierungsdiensten stellen, auch erfüllt werden.

Allgemein bietet Signing Service je nach Vertragsgestaltung und nach Wahl des Teilnehmers fortgeschrittene elektronische Signaturen für natürliche oder juristische Personen sowie qualifizierte elektronische Signaturen für natürliche Personen an. Diese Leistungsbeschreibung beschreibt den Service für elektronische Signaturen für natürliche Personen in der Schweiz.

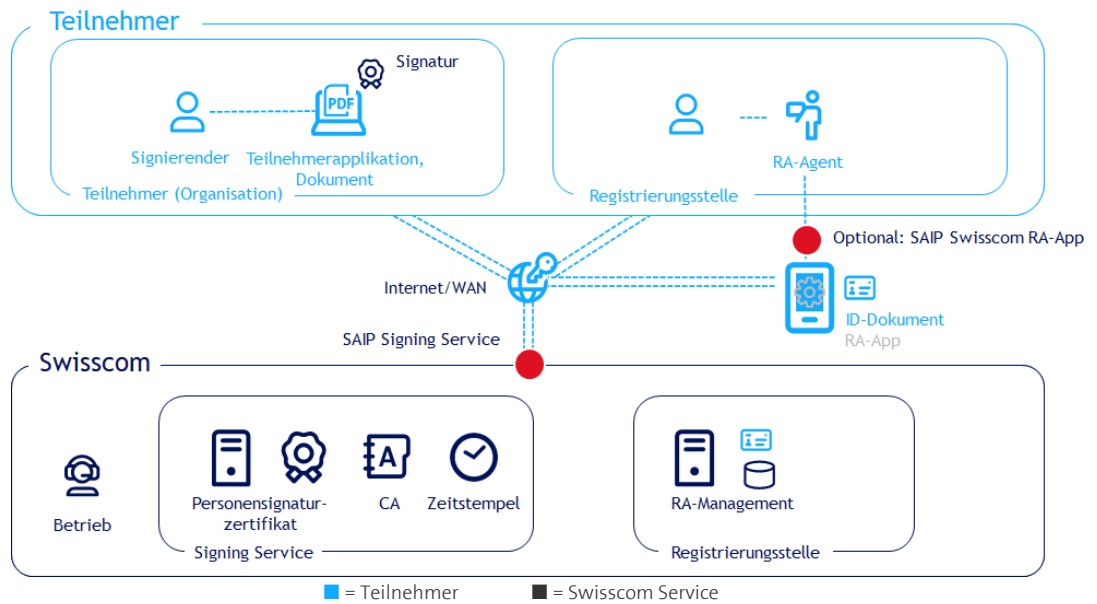


3 Definitionen

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 Leistungsbezügler (Teilnehmer) bereitgestellt, überwacht und die erbrachten Service Level ausgewiesen werden.

Folgende rein schematische Darstellung dient der Veranschaulichung der Leistungen und Leistungs-Komponenten von Signing Service:



Der Übergabepunkt der Leistung ist hierbei für die Signaturen der Anschluss am Internet der Swisscom. 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“:

http://documents.swisscom.com/product/1000255-Digital_Signing_Service/Documents/Reference_Guide/Reference_Guide-All-in-Signing-Service-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

| Standardausprägung | Elektronische Personensignaturen |
|--------------------|---|
| CMS | Cryptographic Message Syntax – Eine im RFC5652 definierte Syntax für die digitale Signatur und kryptographische Mitteilungen |
| CP/CPS | Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten der Klasse "Diamant" (qualifiziert) und „Saphir“ (fortgeschritten). Zertifikatsrichtlinien und Zertifikatspraxis, Dokumente einer Zertifizierungsstelle, die die Richtlinien und Praxis zur Ausstellung von Zertifikaten beschreiben. |
| Distinguished Name | Normierte Form zur Beschreibung eines Zertifikatssubject. Das Subject eines Zertifikates bezeichnet eindeutig die Identifikation des Signierenden. |
| Dokument | Der Begriff Dokument wird, zur besseren Verständlichkeit, synonym für den Begriff Daten benutzt. Es können sowohl Dokumente, als auch Daten signiert werden. |



| Standardausprägung | Elektronische Personensignaturen |
|---|---|
| Elektronische Signatur | Die elektronische Signatur ist ein technisches Verfahren zur Überprüfung der Integrität eines Dokuments, einer elektronischen Nachricht oder anderer elektronischer Daten sowie der Identität des Signierenden. |
| Hash | Eindeutige Abbildung einer grossen Datenmenge auf eine kleine Datenmenge, vergleichbar einem Fingerabdruck eines Dokumentes. Vom Hash können keinerlei Rückschlüsse auf den Dokumenteninhalte gezogen werden. |
| IdP | Identity Provider: In diesem Zusammenhang eine für den Signing Service der Swisscom zugelassene Registrierungsstelle, die nach Audit und Zulassung Registrierungen für Swisscom Signing Service entweder mit eigenem Authentisierungsmittel zur Willensbekundung oder mit einem Standard Authentisierungsmittel der Swisscom Trust Services. |
| 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. |
| Nutzungsbestimmungen (Subscriber Agreement) | Die Nutzungsbestimmungen regeln im Verhältnis zwischen Swisscom (Schweiz) AG und dem Signierenden auf einer Teilnehmerapplikation die Bedingungen für die Nutzung der Signaturzertifikate und Signaturdienstleistung. Diese sind unter https://trustservices.swisscom.com/repository/ abrufbar. |
| OASIS DSS | Schnittstellen Standard für digitale Signaturen für Web Services und andere Services der OASIS Gruppe (Non Profit Organisation für offene Standards in der IT) |
| On-Demand Signature | Häufig in den Technischen Unterlagen verwendeter Begriff für die "Personensignatur" gemäss dieser Leistungsbeschreibung. |
| OTP | One Time Password – Password, welches für eine einmalige Nutzung erzeugt und über SMS übertragen wird. |
| PKCS#1 | Kryptographischer Standard der RSA Laboratories. |
| PWD | Password (-eingabe), für die Authentisierung am Service zu verwendendes Password |
| 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 |
| RA-Service | Service zur Entgegennahme und Archivierung der Identifizierungsdaten, Betrieb in Zusammenhang mit der RA App |
| Registrierungsstelle (RA) | Registrierungsstelle (Registration Authority) Zuständige Stelle für die Identifikation der Signierenden. Kann vom Teilnehmer, Swisscom oder Dritten bereitgestellt werden unter der Voraussetzung eines Vertragsverhältnisses zu Swisscom (Schweiz) AG. |
| REST | Representational State Transfer, Programmierparadigma für verteilte Systeme, insbesondere Webservices. |
| Sichere Signaturerstellungseinheit (HSM) | Qualifizierte und zertifizierte Hardware zur Erstellung von Signaturschlüsseln und Signaturzertifikaten. |



| Standardausprägung | Elektronische Personensignaturen |
|----------------------------|--|
| Signierender | Natürliche Person, die bei vorgängiger Identifikation, Authentifikation und Willensbekundung ein Dokument elektronisch signiert. |
| Smart Registration Service | Service von Swisscom mit Online Identifikationsmethoden, die ebenfalls wie die RA-App die Daten in den RA-Service einspeisen |
| SOAP | Simple Object Access Protocol – Alternatives Schnittstellen Programmierparadigma zu REST für Webservices |
| SSL/TLS | Secure Socket Layer, Transport Layer Security, Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet basierend auf SSL (Zugangs-) Zertifikaten |
| Teilnehmer | Swisscom erbringt die Leistungen gemäss vorliegender Leistungsbeschreibung zu Gunsten des Teilnehmers. Der Teilnehmer ist entweder direkt Kunde von Swisscom mit einem Signing Service Vertrag (inklusive Annahmeerklärung gegenüber Swisscom (Schweiz) AG) oder er hat einen kommerziellen Vertrag mit einem Wiederverkäufer der Swisscom-Leistung mit einer Annahmeerklärung gegenüber Swisscom (Schweiz) AG. |
| Teilnehmerapplikation | Der Teilnehmer gibt den Signierenden Zugang zu einer Applikation, mit der sie elektronische Signaturen gemäss den Nutzungsbestimmungen von Swisscom (Schweiz) AG erstellen können und der Teilnehmer stellt dabei neben der Authentisierung die Übertragung der Signaturdaten zum Fernsignaturservice von Swisscom sicher ("Teilnehmerapplikation"). Die Teilnehmerapplikation nimmt die signierten Daten entgegen und bereitet für den Signierenden das Dokument auf. Der Signaturservice 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. |
| ZertES | Schweizerisches Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate |

4 Ausprägungen und Optionen

| Standardausprägung | Elektronische Personensignaturen |
|---|----------------------------------|
| Qualifizierte elektronische Signatur | ● |
| Fortgeschrittene elektronische Signatur | ● |
| Qualifizierter elektronischer Zeitstempel | ● |
| Identifikation auf Basis von Swisscom Registrierungsstellen/RA-App Identifikationen | ● |
| Identifikation auf Basis von teilnehmereigenen Registrierungsverfahrensidentifikationen | ○ |
| Nutzung von Mobile ID oder Mobile ID App zur Willensbekundung | ● |
| Nutzung von Kombination Passwort / Einmalcode (SMS) zur Willensbekundung | ○ |
| Weitere vom Standard (Mobile ID, Mobile ID App, PWD/OTP) abweichende Willensbekundungsverfahren | ○ |
| Datenaufbewahrung in der Schweiz | ● |
| Betrieb gemäss Zertifikatsrichtlinien (CP/CPS) | ● |
| Nutzung für Signierende mit Wohnsitz in Schweiz, EU und EWR | ● |
| Nutzung für Signierende mit Wohnsitz ausserhalb Schweiz, EU und EWR | ○ |
| Anschluss an Signaturapplikation DocuSign | ○ |



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

4.1 Definition der Leistungen

| Leistung | Definition |
|---|--|
| Qualifizierte elektronische Signatur | Qualifizierte elektronische Signatur gemäss Art. 2 Bst. e ZertES. |
| Fortgeschrittene elektronische Signatur | Fortgeschrittene elektronische Signatur gemäss CP/CPS. |
| Qualifizierter elektronischer Zeitstempel | Qualifizierter elektronischer Zeitstempel gemäss Art. 2 Bst. j ZertES |
| Identifikation auf Basis von teilnehmereigenen Registrierungsverfahren/identifikationen | <p>Optional können auch eigene Identifikationsverfahren des Teilnehmers oder Dritter genutzt werden, wenn diese auditiert und für ZertES zugelassen wurden. Hierzu sind zusätzliche Optionen zur Zulassung dieser Verfahren (Onboarding Support, Audit durch die Anerkennungsstelle) zwingend zu bestellen, sowie eine Option zur Sicherstellung der Konformität während der Nutzungsdauer des Service. Die Optionen sind alle im Servicevertrag oder der Bestellung zusätzlich ausgewiesen und beschrieben. Ebenfalls muss der Teilnehmer oder Dritten als «RA-Stelle» mit Swisscom (Schweiz) AG einen sogenannten «Vertrag zur Delegation der Registrierungsstellentätigkeit» (RA-Delegationsvertrag) abschliessen.</p> <p>Im Rahmen der Sicherstellung der Konformität während der Nutzungsdauer stellt Swisscom Trust Services sicher, dass diese Methoden im Rahmen des jährlichen Wiederholungs- und Surveillanceaudits berücksichtigt werden und Anfragen der Konformitätsbewertungsstelle bzw. Anerkennungsstelle hierzu beantwortet werden. Das beinhaltet auch die Einholung von Angeboten gesonderter Audits durch die Konformitätsbewertungsstelle. Diese Angebote werden dem Kunden oder Resellingpartner zur Annahme und Durchführung vorgelegt. Bei erfolgter Zustimmung führt die Anerkennungsstelle diese Audits durch und Swisscom Trust Services wird anschliessend den von der Anerkennungsstelle eingeforderten Rechnungsbetrag dem Kunden oder Resellingpartner zusätzlich zu den Kosten für Swisscom Trust Services verrechnet. Sollte der Kunden oder Resellingpartner das Audit nicht durchführen wollen und die weitere Anerkennung damit ablehnen, führt das zur Abschaltung der betreffenden Identifikationsmethode im Signatur Service und zur ausserordentlichen Kündigung des Signaturvertrages durch Swisscom Trust Service.</p> |
| Nutzung von Mobile ID oder Mobile ID App zur Willensbekundung | Im Leistungsangebot inbegriffen ist die Nutzung der von Swisscom für alle Mobilfunkteilnehmer in der Schweiz bereitgestellte Mobile ID oder die in der EU/EEA und Schweiz, sowie einzelne weitere Staaten bereitgestellte Mobile ID App. Weitere Informationen hierzu unter https://mobileid.ch |
| Nutzung von Kombination Passwort / Einmalcode (SMS) zur Willensbekundung | Sofern Mobile ID oder Mobile ID App nicht zu Einsatz kommen können für Signaturen, die nicht in einem Fixpreis (Flat) Model pro Signierenden und Monat verrechnet werden auch eine Kombination aus Passwort und Einmalcode zur Verwendung kommen. Diese werden dann bei jeder Signatur abgefragt. Das Passwort wird bei der Registrierung direkt nach Bestätigung der Nutzungsbestimmungen erstmalig gesetzt. Der Einmalcode wird bei jeder Signatur via SMS an die Mobilnummer übermittelt, die bei der Registrierung eingegeben wurde. Im Rahmen von fortgeschrittenen Signaturen reicht auch nur der Einmalcode aus (ein Faktor). |
| Weitere Methoden zur Willensbekundung, die vom Standard abweichen | Optional können auch eigene Authentisierungsverfahren des Teilnehmers oder Dritten zur Willensbekundung des Signierenden genutzt werden, wenn diese auditiert und für ZertES zugelassen wurden, insbesondere im Hinblick auf «sole control», d.h. der Sicherstellung des alleinigen Zugriffs |

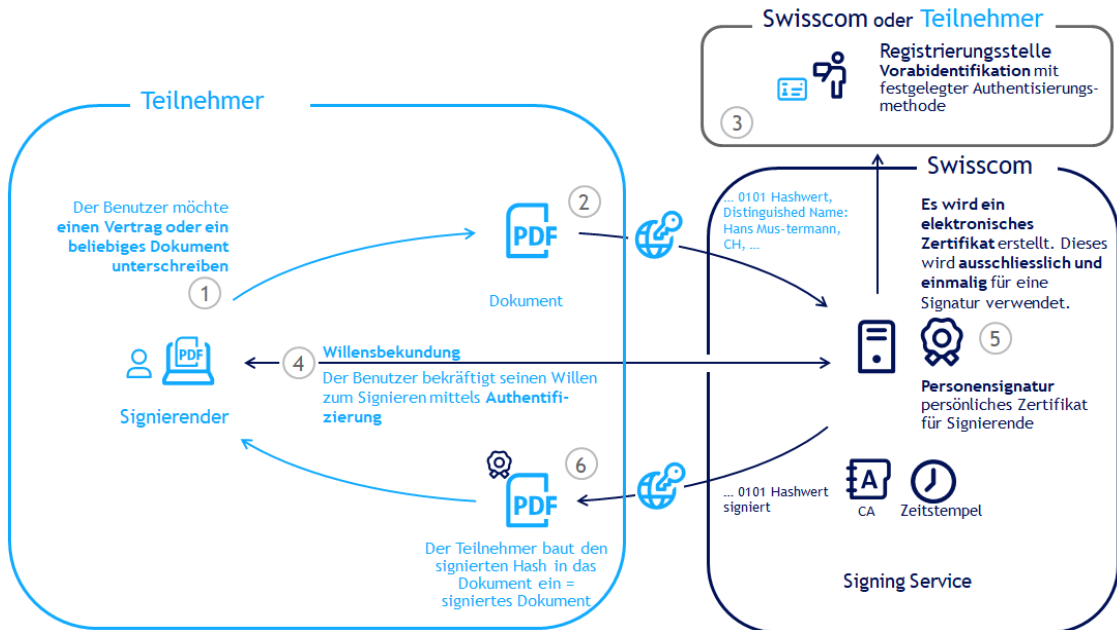


| Leistung | Definition |
|--|---|
| | <p>auf das Signaturzertifikat durch den Signierenden. Swisscom Trust Services wird hier gemäss Bestellformular oder Servicevertrag weitere eigene Verfahren laufend zur Verfügung stellen. Das können auch bereits freigegebene Authentisierungsverfahren anderer Kunden/IdPs sein. Die Nutzung von Authentisierungsverfahren anderer IdPs kann gesonderten Gebühren unterliegen, die diese IdPs von Ihren Nutzern verlangen. Unabhängig davon können auch kundenspezifische Authentisierungsverfahren geprüft und zugelassen werden, z.B. kundeneigene Apps. Hierzu sind zusätzliche Optionen zur Zulassung dieser Verfahren (Onboarding Support, Audit durch die Anerkennungsstelle) zu bestellen, sowie eine Option zur Sicherstellung der Konformität während der Nutzungsdauer des Service. Die Optionen sind alle im Servicevertrag oder der Bestellung zusätzlich ausgewiesen und beschrieben. Im Rahmen der Sicherstellung der Konformität während der Nutzungsdauer stellt Swisscom Trust Services sicher, dass diese Methoden im Rahmen des jährlichen Wiederholungs- und Surveillanceaudits berücksichtigt werden und Anfragen der Konformitätsbewertungsstelle bzw. Anerkennungsstelle hierzu beantwortet werden. Das beinhaltet auch die Einholung von Angeboten besonderer Audits durch die Anerkennungsstelle. Diese Angebote werden dem Kunden oder Partner zur Zustimmung der Durchführung vorgelegt. Bei erfolgter Zustimmung führt die Anerkennungsstelle diese Audits durch und Swisscom Trust Services wird anschliessend den von der Anerkennungsstelle eingeforderten Rechnungsbetrag dem Kunden oder Partner zusätzlich zu den Kosten für diese Option verrechnen. Sollte der Kunde das Audit nicht durchführen wollen und die weitere Anerkennung damit ablehnen, führt das zur Abschaltung der betreffenden Authentisierungsmethode im Signatur Service und zur automatischen Beendigung des Signaturvertrages.</p> |
| <p>Datenaufbewahrung in der Schweiz</p> | <p>Die Datenaufbewahrung mit den Personendaten aus den Zertifikaten findet nur in der Schweiz im Einklang mit den einschlägigen Vorschriften der schweizerischen Datenschutzgesetzgebung statt.</p> |
| <p>Betrieb gem. Zertifikatsrichtlinien (CP/CPS)</p> | <p>Der Betrieb eines Zertifizierungsdiensteanbieter richtet sich nach den Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten der Klasse "Diamant" (qualifiziert) und „Saphir“ (fortgeschritten). Diese können in der aktuellen Fassung hier aufgerufen werden: https://trustservices.swisscom.com/repository/</p> |
| <p>Nutzung für Signierende mit Wohnsitz in Schweiz, EU und EWR</p> | <p>Die Nutzungsbestimmungen genügen rechtlich nur den Anforderungen für Signierende mit Wohnsitz in der Schweiz, EU und EWR.</p> |
| <p>Nutzung für Signierende mit Wohnsitz ausserhalb der Schweiz, EU und EWR</p> | <p>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 des Authentisierungsmittels und der Verschlüsselungsanforderungen) geprüft werden. Ggfs. müssen die Nutzungsbestimmungen aufgrund der konsumentenrechtlichen Regelungen dafür angepasst werden und die technischen Authentisierungsmöglichkeiten überprüft und bereitgestellt werden. Das ist nach Absprache und gegen gesondertes Angebot der Swisscom Trust Services AG möglich.</p> |
| <p>Anschluss an Signaturapplikation DocuSign</p> | <p>Im Falle dieser Option nutzt der Teilnehmer DocuSign als Signaturapplikation, welche selbst eine Schnittstelle für Fernsignaturservices vorsieht. Swisscom bietet optional einen Connector an, der das DocuSign Interface an das Interface des Swisscom Signing</p> |



| Leistung | Definition |
|----------|--|
| | Service anbietet und somit fortgeschrittene und qualifizierte Signaturen mit der DocuSign Applikation erlaubt. |

4.1.1 Ablauf der Signaturerstellung für alle Optionen



- Applikation des Teilnehmers ist unter Verwendung eines SSL/TLS Zugangszertifikat mit der Swisscom Signing Service Plattform verbunden.
- Der Signierende, der bereits für den Service direkt oder via Identity Provider (IdP) identifiziert wurde, loggt sich in seine Teilnehmerapplikation ein (1) und wählt das zu signierende Dokument aus. Die Teilnehmerapplikation bildet einen Hash nach Vorgaben von Swisscom (2) und sendet ihn an die Signing Service Plattform. Weiterhin werden auch für das Signaturzertifikatsubjekt relevante Angaben (Distinguished Name) von der Teilnehmerapplikation übergeben.
- Sofern die Registrierungsstelle der Swisscom (Schweiz) AG mit der RA-App oder der Smart Registration Service genutzt wurde, erfolgt ein Abgleich der mit vom Signierenden übermittelten Signaturdaten mit den Identifikationsdaten der Swisscom Registrierungsstelle. (3)
- Sofern der Teilnehmer von der Registrierungsstelle erfasst und für die Signatur zugelassen ist, fordert der Signing Service die Willensbekundung des Signierenden an. (4)
- Die Willensbekundung des Signierenden mittels des während der Registrierung festgelegten Authentisierungsmittels wird ausgelöst. Qualifizierte Zertifikate und Signaturen werden ausschliesslich auf Basis einer 2-Faktor Authentisierung erstellt, fortgeschrittene Signaturen können auch mit einer 1-Faktor Authentisierung ausgestellt werden.
- Erstellung und Nutzung von Schlüsselmaterial (private und öffentliche Schlüssel) sowie von Zertifikaten, welche für die fortgeschrittene bzw. qualifizierte elektronische Signatur (inkl. nach ZertES qualifiziertem Zeitstempel) notwendig sind. (5) Das Schlüsselmaterial wird auf der Signing Service Plattform bei Swisscom erzeugt und verwendet. Zu diesem Schlüsselpaar wird ein entsprechendes fortgeschrittenes bzw. qualifiziertes Zertifikat gemäss den Zertifikatsrichtlinien der Swisscom (Schweiz) AG und dem von der Teilnehmerapplikation übergebenen Subjekt des Zertifikates (Distinguished Name) ausgestellt. Das Zertifikat und das Schlüsselpaar werden für einen einzigen Signaturauftrag des Teilnehmers verwendet und das



Schlüsselpaar nach dessen Verwendung gelöscht. Persönliche Zertifikate sind grundsätzlich für wenige Minuten gültig.

- Signierung des Hash-Wertes (kryptographische Prüfsumme über einen Datensatz/Text beliebiger Länge), um dessen Integrität sicher zu stellen nach CMS oder PKCS#1 Standard.
- Rückgabe der Signatur sowie von zusätzlichen Validierungsinformationen im Zertifikat (z.B. Zertifikatskette zum vertrauenswürdigen Root-Zertifikat sowie qualifizierter Zeitstempel). Die Teilnehmerapplikation stellt die Signatur des Dokumentes aufgrund des signierten Hashs sicher. (6)

4.2 Prozesse und Tools zur Personenidentifikation (Registrierungsstelle)

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

- Der Teilnehmer kann in die Lage versetzt werden, für Swisscom lokal selbst Kollegen, Kunden und Partner im face2face Verfahren zu identifizieren. Hierfür kann er die RA-App einsetzen. Diese ist gesondert zu bestellen und in einer gesonderten Leistungsbeschreibung beschrieben.
- Der Teilnehmer kann Identifikationsverfahren nutzen, die Swisscom oder Partner im Rahmen von Smart Registration Service als Fernidentifikationsverfahren anbietet. Diese werden in einer gesonderten Leistungsbeschreibung beschrieben und müssen gesondert bestellt werden.
- Swisscom bietet die Registrierungsmöglichkeiten des Smart Registration Service auch direkt zum Bezug über Gutscheincodes oder Direktbezahlung über die Webseite <https://srsident.trustservices.swisscom.com> an.
- IdPs können ihren Nutzern oder über den Smart Registration Service ebenfalls Registrierungen mit Authentifizierungsmittel anbieten, die auch in anderen Signaturapplikationen zur Willensbekundung eingesetzt werden. Hierbei erfolgt das Angebot entweder durch den IdP oder im Rahmen des Smart Registration Service.
- Der Teilnehmer kann Registrierungen nutzen, die Swisscom vor Ort in den Swisscom Shops anbietet.
- Der Teilnehmer kann seine eigenen Identifikationsmethoden nutzen und selbst eine Registrierungsstelle mit projektspezifischer Identifizierung aufbauen («IdP»). Dieses Vorgehen ist vorgängig mit Swisscom abzustimmen und im Rahmen eines Signing Onboarding Projektes zu erarbeiten. Hierzu muss der Teilnehmer ein Umsetzungskonzept vorlegen, welches durch Swisscom geprüft und bewertet wird. In der Regel müssen für Teilnehmer individualisierte Registrierungsstellenprozesse zusätzlich von der Anerkennungsstelle oder Konformitätsbewertungsstelle für Zertifizierungsdienste freigegeben werden. Die Registrierungsdaten können je nach Ausprägung beim Teilnehmer verbleiben oder auch bei Swisscom in den Smart Registration Service transferiert werden. Hierzu ist eine gesonderte Bestellung notwendig.

Alle Identifikationsverfahren und Registrierungen sind nicht Bestandteil dieser Leistungsbeschreibung.

4.2.1 Prozess zur Organisationsprüfung

Sofern bei dem vorgenannten Verfahren zur Personenidentifikation auch die mit der Person verbundene Organisation festgehalten wird, so wird eine Organisationsprüfung gemäss Bestimmung der CP/CPS vor Aufnahme des Service von Swisscom überprüft. Hierzu muss diese 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.

4.3 Datenablage und Verantwortlichkeiten

Mit der Nutzung der von Swisscom zur Verfügung gestellten RA-App, der von Partner angebotenen Fernidentifikationen des Smart Registration Service werden die Daten zur identifizierten Person sowie die Identifikationsunterlagen und der Nachweis der Annahme der Nutzungsbestimmungen ausschliesslich auf Swisscom Servern in der Schweiz gespeichert und entsprechend den Fristen gemäss CP/CPS oder gemäss Gesetz aufbewahrt. Das gilt nicht für die Daten eines IdP – hier gelten die Regeln des IdPs. Die Aufnahme der Daten hingegen kann je nach Situation (z.B. bei Auslandseinsatz der RA-App) auch ausserhalb erfolgen.

Bei projektspezifischen Verfahren wird die Speicherung und der Speicherort in der gesonderten Vereinbarung zur Delegation der Personenidentifikation mit Umsetzungskonzept festgehalten.



4.4 Willensbekundung

Jede persönliche Signatur bedingt die Abgabe einer Willensbekundung durch den Signierenden. Für die Willensbekundung wird in der Regel das Gerät (z.B. Mobiltelefon mit der Mobiltelefonnummer oder Smartphone) verwendet, das bei der Identifikation des Signierenden eingesetzt wurde.

Für die Abgabe der Willensbekundung selbst stehen derzeit verschiedene Verfahren zur Verfügung:

- **Mobile ID:** Derzeit nur einsetzbar mit MobileID-fähigen SIM-Karten von Schweizer Mobiltelefonnummer. Hierdurch kann sich der Signierende für eine Signatur mittels direkter 2-Faktor Authentisierung authentisieren und eine Willensbekundung zur Signatur auslösen. Sollte Mobile ID bei der Mobiltelefonnummer nicht verfügbar sein, wird automatisch auf das Mobile ID App oder PWD/OTP Verfahren zurückgegriffen. Mobile ID muss vor Benutzung initialisiert werden.
- **PWD/OTP:** Hierbei authentifiziert sich der Signierende über eine Passwortheingabeseite, die er von der Signaturapplikation erhält, beim Signing Service und löst bei dem Service die Generierung eines Einmalcodes aus, der über SMS an das Mobiltelefon des Signierenden übermittelt wird. Dieses gibt der Signierende in die Teilnehmerapplikation ein.
- **Mobile ID App:** Diese Authenticator App kann genutzt werden, solange nicht das Standard Mobile ID Verfahren im Einsatz ist. Es ist ebenfalls auch für den internationalen Einsatz ausserhalb der Schweiz geeignet. Der Signierende löst eine 2-Faktor Authentisierung mittels eines vom Gerät ermöglichten biometrischen Merkmals oder eines PINs/Passwords. Hierfür muss die App vor dem ersten Einsatz, z.B. vor der Bestätigung der Nutzungsbestimmungen, installiert werden und mit der Mobilnummer initialisiert werden. Es ist ein Smartphone notwendig, welches mit dem Internet verbunden ist.
- **OTP:** Bei diesem Verfahren entfällt die Authentisierung des Signierenden beim Signing Service, sondern der Signierende sendet direkt an den Signing Service ein Einmalcode, das ihm zuvor via SMS übersendet wurde. Dieses Verfahren kann nur für fortgeschrittene Signaturen verwendet werden.
- **Projektspezifische Willensbekundung:** Sollen die voran genannten Verfahren nicht zu Einsatz kommen, so sind etwaige projektspezifische Willensbekundungsverfahren mit Swisscom vorab abzustimmen. Hierzu muss der Teilnehmer vorgängig zum Abschluss des Vertrages ein Umsetzungskonzept vorlegen, welches durch Swisscom geprüft und bewertet wird. In der Regel müssen für Teilnehmer individualisierte Willensbekundungsprozesse zusätzlich von der Anerkennungsstelle oder Konformitätsbewertungsstelle für Zertifizierungsdienste freigegeben werden.
- **IdP Verfahren:** diese Verfahren wurden als projektspezifische Willensbekundung von Swisscom freigegeben. Die Methoden sind von IdP zu IdP unterschiedlich und der Nutzer muss sich für die Beschreibung der Verfahren an den jeweiligen IdP (z.B. Bank) wenden, die dieses Verfahren seinen Kunden und Nutzern anbietet.

4.5 Option: Nutzung von DocuSign

Sofern der DocuSign Connector eingesetzt wird, kann der Teilnehmer auch mit DocuSign fortgeschritten oder qualifiziert signieren. Diese Option funktioniert nur mit Verfahren, die auf Standard-Willensbekundungsmethoden von Swisscom aufsetzen und Identifikationen nutzen, die von Swisscom Verfahren durchgeführt werden oder bei denen die Registrierungsdaten durch den Smart Registration Service verwaltet werden.

Die DocuSign Applikation muss hierzu mit einem sogenannten «Swisscom Pen» erweitert werden, einem Auswahl-feld in der Benutzeroberfläche von DocuSign, welches die Eingabe der Mobilfunknummer des Signierenden und die Auswahl der Signaturqualität (fortgeschritten/qualifiziert) ermöglicht.

Das von DocuSign signierte Dokument enthält nach erfolgreicher Signatur nicht nur das Siegel von DocuSign sondern auch die entsprechende Personensignatur mit einem Swisscom Zertifikat. Für die Signatur ist eine Willensbekundung (PWD/OTP oder Mobile ID, Mobile ID App) abzugeben. Das setzt eine einmalige Vorabregistrierung voraus.

5 Leistungsdarstellung und Verantwortlichkeiten

5.1 Signaturservice

Einmalige Leistungen



| Tätigkeiten (S = STS/T = Teilnehmer) | S | T |
|---|---|---|
| Bereitstellung des Service | | |
| 1. Sicherstellung der Registrierung der Signierenden (z.B. Bestellung einer Registrierung bei Swisscom). 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 der Schnittstelle SAIP basierend auf OASIS DSS Protokoll über SOAP oder REST bzw. ETSI EN 119 432 Standard angepasst für die Nutzung kurzlebiger Signaturzertifikate. Die Schnittstelle ist unter http://documents.swisscom.com/product/1000255-Digital_Signing_Service/Documents/Reference_Guide/Reference_Guide-All-in-Signing-Service-en.pdf abrufbar. | ✓ | |
| 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 Reference Guide, Unterpunkt 3. | | ✓ |
| 5. Zusenden der unterzeichneten Annahmeerklärung mit den regulatorisch notwendigen Informationen. | | ✓ |
| 6. Option "Organisationseintrag im Signaturzertifikat": Bereitstellung auf Anforderung von Swisscom 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. | | ✓ |
| 7. Option "Organisationseintrag im Signaturzertifikat": Prüfung der Berechtigung zum Führen des Organisationsnamens im Zertifikat. | ✓ | |
| 8. Zusenden eines öffentlich vertrauenswürdigen (notwendig im Falle der ETSI Schnittstelle) oder selbst signierten SSL/TLS-Authentisierungszertifikat zur Authentisierung gegenüber dem Signing Service Server und zur verschlüsselten Kommunikation mit dem Signing Service. Spezifikation siehe Annahmeerklärung. | | ✓ |
| 9. Freischaltung der Kommunikation für das zugesendete Authentisierungszertifikat. | ✓ | |
| 10. Ggfs. Konfiguration der Firewall, serverseitig beim Teilnehmer. | | ✓ |
| 11. Benennung eines Verantwortlichen inklusive laufender Stellvertretung für alle Fragen bezüglich der Technik, Sicherheit und Durchführung der Registrierung von Signierenden und Ansprechpartner für Auditfragen. | | ✓ |
| 12. Aufschalten des Teilnehmers und Zusenden der teilnehmerspezifischen Zugangsdaten. | ✓ | |
| 13. Einbindung des Signing Service Services in die teilnehmerspezifische Anwendung(en) bzw. teilnehmerseitige Anbindung der Schnittstelle zum Signing Service, z.B. durch Einsatz einer Partnerapplikation. | | ✓ |
| 14. Prüfung des Zugriffs auf den Signing Service Server und der Ausstellung von Signaturen. Umgehende Meldung allfälliger Fehler, bevor die Signaturen benutzt werden. | | ✓ |
| 15. Fehlerbehebung durch Update oder Neuinstallation. | ✓ | |
| 16. 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. | ✓ | |
| 2. Löschen der Schlüssel aus dem HSM. | ✓ | |



Wiederkehrende Leistungen

| Tätigkeiten (S = STS/T = Teilnehmer) | S | T |
|--|---|---|
| Standardleistungen | | |
| 1. Betrieb der Signing Service Infrastruktur. | ✓ | |
| 2. LifeCycle Management der Signing 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 Swisscom, sofern von Swisscom oder der Anerkennungsstelle von Swisscom (Schweiz) AG verlangt. | | ✓ |
| 5. Anpassung der Definition der Sicherheitsanforderungen. | ✓ | |
| 6. Lifecycle-Management seines SSL/TLS-Authentisierungszertifikates rechtzeitiger Austausch bei Ablauf der Gültigkeit durch den benannten Sicherheitsverantwortlichen durch E-Mail an sts.sale-support@swisscom.com unter Bezeichnung des Kontonamens. Vermeidung jeglichen Aufbrechens der SSL/TLS Verbindung (z.B. durch "Inspection" Module). | | ✓ |
| 7. Erstellung von Signaturzertifikaten nach dem Standard X.509. | ✓ | |
| 8. Festlegung der Signaturzertifikatsinhalte und Verfahren zur Signaturerstellung. | ✓ | |
| 9. Sicherstellung des Einsatzes von technischen Authentifikationsmitteln und vertraglich vereinbarter Authentifizierungsmethode (z.B. Mobile ID, Mobile ID App, PWD/OTP, etc.). | | ✓ |
| 10. Sicherstellung vorab, dass nur diejenigen Signierenden an der Signatur teilnehmen (z.B. durch Prüfung mittels eines von der API zur Verfügung gestellten Verifizierungscalls), die mit den entsprechenden Authentifizierungsmittel für die Signaturart registriert und zugelassen sind, sonst erfolgt eine Fehlermeldung oder optional Weiterleitung zum Identifizierungsdienst | | ✓ |
| 11. Ansprache des registrierten Authentisierungsmittels, sofern in der Signaturanfrage ein registrierter Hinweis auf den Signierenden (z.B. Mobilnummer, uuid, E-Mail etc.) mitgegeben wird. | ✓ | |
| 12. Durchführen von Signaturen, für die eine Willensbekundung des Signierenden vorliegt. | ✓ | |
| 13. Signatur in Verbindung mit einem qualifizierten Zeitstempel nach ZertES wird angeboten. | ✓ | |
| 14. Sicherstellen der Mitwirkungsleistungen und Auflagen durch den Sicherheitsverantwortlichen. | | ✓ |
| 15. Bereitstellung der Supportdienstleistungen (Service Desk, Incident Management usw.) | ✓ | |
| 16. Zählung aller Signaturanfragen gemäss dem Verrechnungsmodell und summarische Verrechnung an den Teilnehmer | ✓ | |
| 17. Errichtung eines Abrechnungssystems und Zählung aller Signaturanfragen und Verrechnung mit dem Signierenden bzw. Zuordnen von Signaturfragen zu unterschiedlichen Endkunden des Teilnehmers | | ✓ |
| 18. Melden von Mutationen der teilnehmerspezifischen Informationen (Kontaktpersonen, SSL/TLS Zertifikat usw.) | | ✓ |
| 19. Nachführen der teilnehmerspezifischen Informationen (Kontaktpersonen, SSL/TLS Zertifikat usw.) | ✓ | |
| 20. Melden von Sicherheitsvorfällen auf dem System der Teilnehmerapplikation, die den Signing Service Service betrifft. | | ✓ |
| 21. Melden von Sicherheitsvorfällen auf dem System des Signaturservice, die Auswirkung auf den Teilnehmer hat. | ✓ | |
| 22. Entscheid und Verantwortung für rechtliche Wirkungen der gewählten Signaturart (vgl. Kapitel 8.1) | | ✓ |
| 23. Hinweis an die Signierenden über die verwendete Signaturart in der Benutzeroberfläche der Teilnehmeranwendung oder in der Frage der zur Willensbekundung | | ✓ |



| Tätigkeiten (S = STS/T = Teilnehmer) | S | T |
|--|---|---|
| 24. Anzeige an den Signierenden, ob es sich um eine fortgeschrittene oder qualifizierte Signatur handelt | | ✓ |
| 25. Anpassung der Schnittstelle an die neuen Vorgaben von Swisscom binnen von 3 Monaten. | | ✓ |

5.2 Abrechnungsmodell «Vergütung pro aktiv Signierenden»

Sofern der Teilnehmer eine Abrechnung gemäss dem Vergütungsmodell «Vergütung pro aktiv Signierenden» wünscht (siehe 7.1.2) sind zusätzliche Verpflichtungen einzugehen, da dieses Verfahren nur bestimmte im Servicevertrag benannte Authentisierungsverfahren zulässt.

| Tätigkeiten (S = STS/T = Teilnehmer) | S | T |
|---|---|---|
| Leistungen bei Nutzung des Vergütungsmodells «Vergütung pro aktiv Signierenden» | | |
| 1. Der Teilnehmer muss vor der Teilnahme an einer Signatur sicherstellen, dass der Signierende über die in diesem Verfahren gemäss Servicevertrag vorgeschriebene Authentisierungsmethode(n) verfügt. Das kann z.B. mit geeigneten API-Aufrufen (z.B. «VerifyCall») geschehen, die anzeigen, mit welchen Authentisierungsverfahren der Signierende registriert wurde. | | ✓ |
| 2. Sofern der Signierende nicht über die zugelassene Authentifizierungsmethode verfügt, muss der Teilnehmer dem Signierenden eine aussagekräftige Rückmeldung über die Ablehnung zum Signaturverfahren geben und ihm z.B. aufzeigen, wie eine neue Registrierung mit anderen Authentisierungsverfahren erfolgen kann. Alternativ kann er ihm auch die Möglichkeit geben über einen weiteren Zugang (ClaimedID) zum Signing Service eine Signatur nach einem anderen Abrechnungsmodell zu ermöglichen. | | ✓ |
| 3. Der Teilnehmer muss nach seinem Vermögen sicherstellen, dass durch die Wahl des Vergütungsmodells und der Fehlnutzung durch nicht zugelassene Authentisierungsmethoden keine Supportaufwände bei Swisscom entstehen. Bei hierdurch erhöhtem Supportaufwand behält sich Swisscom vor, nach zweimaliger Mahnung die Supportaufwände zu berechnen oder das Vergütungsmodell nach Absprache mit dem Teilnehmer auf ein anderes Vergütungsmodell umzustellen. | | ✓ |



5.3 Option: Swisscom DocuSign Connector

| Tätigkeiten (S = STS/T = Teilnehmer) | S | T |
|--|---|---|
| Leistungen bei optionaler Nutzung des DocuSign Connectors | | |
| 1. Sicherstellung der Registrierung der Signierenden (z.B. über Swisscom Shops oder zusätzlichen Verträgen zur Registrierung, z.B. RA-App) | | ✓ |
| 2. Sicherstellung der Bereitstellung und Parametrisierung durch DocuSign: <ul style="list-style-type: none"> Übermittlung der korrekten DocuSign Account ID an Swisscom in der Bestellung. Der Teilnehmer bestellt bei DocuSign nach der Bestellung bei Swisscom das «DocuSign Express SKU» Der Teilnehmer löst ein Ticket bei DocuSign aus (https://support.docusign.com/en/articles/How-Do-I-Open-a-Case-in-the-DocuSign-Support-Center) und bestellt die Parametrisierung des „Swisscom Pen“ (visuelles Auswahlfeld der Swisscom Signatur in der DocuSign Oberfläche). Die Pen ID Nummer lautet: Swisscom fortgeschrittene Signatur Schweiz: 954 Swisscom qualifizierte Signatur Schweiz: 952 | | ✓ |
| 3. Information an Swisscom, sofern die DocuSign Installation mit «DocuSign Express SKU» und «Swisscom PEN» durch DocuSign eingerichtet wurde und für die Integration des Swisscom DocuSign Connectors bereit steht | | ✓ |
| 3. Anschluss des DocuSign Connectors an den Signing Service von Swisscom für die genannte Account ID. | ✓ | |

5.4 Option: Eigene Identifikations- und/oder Authentisierungsmethode

| Tätigkeiten (S = STS/T = Teilnehmer) | S | T |
|--|---|---|
| Leistungen bei optionaler Nutzung von eigenen Identifikations- und/oder Authentisierungsverfahren | | |
| 1. Sicherstellung der Erstauditierung: Bestellung der notwendigen zusätzlich kostenpflichtigen Optionen (Onboarding Support) für das Review und Abnahme eines Umsetzungskonzeptes sowie die notwendige Auditierung der delegierten RA-Stelle durch eine Konformitätsbewertungsstelle bzw. Auditor. (Siehe Leistungsbeschreibung "Onboarding Support"). | | ✓ |
| 2. Vorlage eines RA Delegationsvertrages auf Basis Umsetzungskonzept. | ✓ | |
| 3. Erstellen eines Umsetzungskonzeptes durch die delegierte RA-Stelle. Abschliessen eines RA-Delegationsvertrages der delegierten RA-Stelle mit Swisscom (Schweiz) AG. | | ✓ |
| 4. Vorlage der Verfahren bei den jährlichen Wiederholungs- bzw. Surveillanceaudits bei den Auditoren, die entsprechend über weitere kostenpflichtige Audits entscheiden. | ✓ | |
| 5. Regelmässige Teilnahme der delegierten RA-Stelle am jährlichen Wiederholungs- bzw. Surveillanceaudit, soweit vom Auditor gefordert sowie gesonderte Beauftragung des Wiederholungs- und Surveillanceaudits nach Angebot, welches Swisscom Trust Services AG beim Auditor zuvor einholt und vom Teilnehmer bestätigen lässt. | | ✓ |

5.5 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. | ✓ | |



| Tätigkeiten (S = STS/T = Teilnehmer) | S | T |
|---|---|---|
| 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: <ul style="list-style-type: none"> • Anpassung der Nutzungsbestimmungen im Hinblick Konsumenten- und Datenschutz • Erfüllung der Datenschutzaufgaben des Wohnsitzlandes (z.B. Pflege eines speziellen Datenverarbeitungsverzeichnisses, Stellen eines Datenschutzbeauftragten, etc.) • Konfiguration im Hinblick auf erlaubte Kryptoalgorithmen • Erfüllung der Auflagen für den Einsatz des Authentisierungsmittels 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 Datenschutzerfordernungen nicht erfolgen können (z.B. kein Einsatz der RA-App) sondern nur Fernregisrierungen möglich sind (z.B. Videoidentifikation), sofern zugelassen. | | ✓ |
| 5. Akzeptanz, dass der Zertifizierungsdienst 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: <ul style="list-style-type: none"> • Z.B. Einschränkung des zu verwendenden Authentisierungsverfahrens (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. <ul style="list-style-type: none"> • 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 der Mobile ID App 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 Authentisierungsmethoden 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 9, Beauftragung der notwendigen Änderungen oder Einstellung des Signaturservices für Signierende dieses RoW Wohnsitzlandes gemäss Fristsetzung. | | ✓ |



6 Service Level und -Reporting

6.1 Service Levelpr

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 3) erbracht. Bei mehreren möglichen Service Levels pro Ausprägung erfolgt die Auswahl des Service Levels im Servicevertrag.

| Service Level & Zielwerte | | | Elektronische Personensignaturen |
|---|---------------------|---|----------------------------------|
| 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 | ● |
| 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.

● = Standard (im Preis inbegriffen)

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 Rechnungsstellung und Mengenreport

7.1 Rechnungsstellung

Die Details zur Rechnungsstellung werden im Service Vertrag geregelt. Grundsätzlich gibt es drei Verrechnungsverfahren:

7.1.1 Vergütung nach Abruf - Postpaid Modell

Hierbei werden im Nachgang die abgerufenen Mengen des letzten Leistungszeitraumes gezählt und mit dem für diese Bezugsmenge vorgesehenen Preis im Servicevertrag verrechnet. Bei diesem Verrechnungsverfahren können beliebige im Servicevertrag zugelassene Authentisierungsverfahren zur Signaturfreigabe genutzt werden.

7.1.2 Vergütung pro aktiv Signierendem – Postpaid Modell

Hierbei werden im Nachgang die Anzahl der im letzten Leistungszeitraum aktiv Signierenden gezählt und mit der für ihre Anzahl vorgesehenen Preis im Servicevertrag verrechnet. Hierbei kann es pro Signierenden eine maximale Anzahl von zugelassenen Signaturen pro Leistungszeitraum geben. Überschüssige Signaturen werden dann einzeln gemäss dem Modell von 7.1.1 mit dem für diese Bezugsmenge vorgesehenen Preis verrechnet. Dieses Verfahren ist nur eingeschränkt nutzbar für bestimmte Authentisierungsmethoden und unterliegt für den Teilnehmer besonderen Verpflichtungen nach 5.2.

7.1.3 Vergütung nach volumengebundenen Nutzungspreismodell – Prepaid Modell

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 des Volumens ist unter gewissen Umständen während der Vertragslaufzeit durch Abschluss eines Neuvertrages möglich.

7.2 Mengenreport

Mengenreports werden im Servicevertrag geregelt. Anonymisierte Reports mit allen Signaturabfragen zu einem Leistungsmonat können auf Bedarf zur Klärung von Problemen angefragt werden. Swisscom behält sich vor, bei regelmässigen Anfragen die Lieferung der Einzelleistungsreports in Rechnung zu stellen.

8 Besondere Regelungen

8.1 Teilnehmerapplikation

Die Teilnehmerapplikation ist nicht Bestandteil dieser Leistungsbeschreibung. Sie wird durch den Teilnehmer selbst, durch einen Swisscom Partner oder Swisscom selber beigestellt.

8.2 Signaturarten 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 übernimmt hierfür keine Verantwortung:

Qualifizierte elektronische Signatur (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 abweichende gesetzliche oder vertragliche 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.

Fortgeschrittene elektronische Signatur (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.

Je nach Situation benötigen gewisse Dokumente also die handschriftliche Unterschrift oder die QES 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 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 Swisscom im Auftrag des Signierenden übermittelten Signaturanfragen (Teilnehmerdaten) werden grundsätzlich von Swisscom mit der Muttergesellschaft Swisscom (Schweiz) AG 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.
- Der 3rd Level Support des Applikationsherstellers hat in Supportfällen aus der EU temporären VPN-Zugriff auf Applikationsdaten bei Swisscom, 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 SSL Zertifikat) für diese Dritte ersichtlich sein. Der Zugriff wird von einem Swisscom-Techniker 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, welche die Konformität der Signaturanwendung bestätigen müssen, können im Rahmen von Audits unter Aufsicht von Swisscom 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.