



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

Leistungsbeschreibung Siegel CH (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 | 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 | 6 |
| 4.2 | Ablauf der Siegelerstellung..... | 7 |
| 4.3 | Prozess zur Prüfung eines Siegelerstellers..... | 8 |
| 4.4 | Revokation (Ungültigkeitserklärung) eines Siegelzertifikates | 8 |
| 5 | Leistungsdarstellung und Verantwortlichkeiten | 8 |
| 6 | Service Level und -Reporting | 10 |
| 6.1 | Service Level | 10 |
| 6.2 | Service Level Reporting | 11 |
| 7 | Rechnungsstellung und Mengenreport | 11 |
| 7.1 | Rechnungsstellung..... | 11 |
| 7.2 | Mengenreport | 11 |
| 8 | Besondere Regelungen | 12 |
| 8.1 | Teilnehmerapplikation..... | 12 |
| 8.2 | Betrieb der Teilnehmerapplikation, wenn Teilnehmer und Siegelersteller nicht identisch sind | 12 |
| 8.3 | Einsatzmöglichkeiten des fortgeschrittenen oder geregelten elektronischen Siegels | 12 |
| 8.4 | Datenbearbeitung durch Dritte aus dem In- oder Ausland, Notfallzugriffe | 12 |



2 Übersicht zum Service

Der Signing Service ist eine serverbasierte Fernsignatordienstleistung vertrieben durch Swisscom Trust Services AG und erbracht durch die Swisscom (Schweiz) AG in den Rechenzentren der Schweiz. 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.

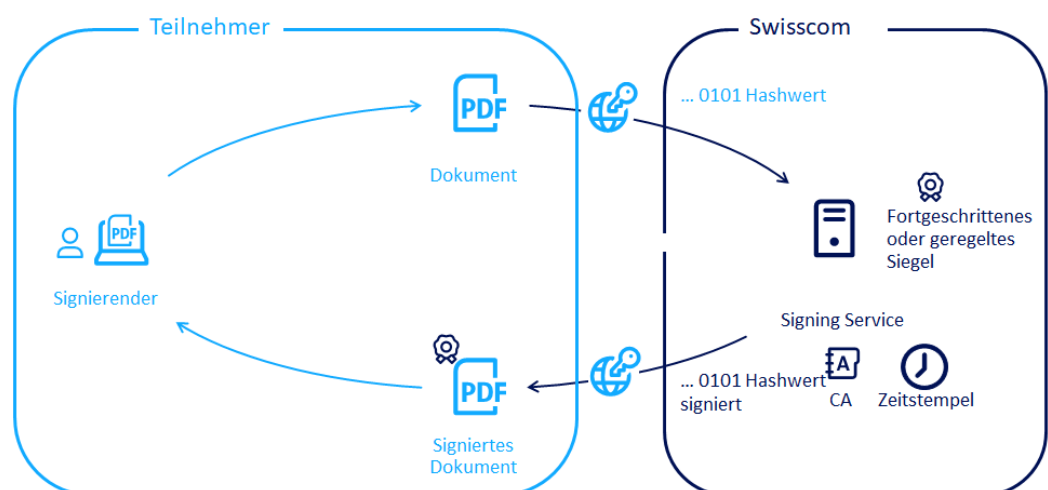
Swisscom (Schweiz) AG ist in der Schweiz gemäss ZertES anerkannte Anbieterin von Zertifizierungsdiensten im Bereich der elektronischen Signatur. Eine akkreditierte Anerkennungsstelle prüft regelmässig, ob die Anforderungen, die das schweizerische Recht und / oder technische Normen an eine anerkannte Anbieterin von Zertifizierungsdiensten im Bereich der elektronischen Signatur stellt, auch erfüllt werden.

Allgemein bietet der Signing Service je nach konkreter Vertragsgestaltung fortgeschrittene und qualifizierte elektronische Signaturen für natürliche Personen sowie fortgeschrittene und geregelte elektronische Siegel für Organisationen an. Vorliegende Leistungsbeschreibung beschreibt den Service einerseits für fortgeschrittene elektronische Siegel und andererseits für geregelte elektronische Siegel für Organisationen im Sinne der schweizerischen Gesetzgebung (ZertES).

Die Fernsignatordienstleistung wird Teilnehmern zur Verfügung gestellt, die eine Teilnehmerapplikation betreiben. Siegelerstellende Organisationen (nachfolgend "Siegelersteller", vgl. hierzu die detaillierte Definition unter Ziffer 2) können mit Signing Service ein elektronisches Siegel auf digitale Dateien anbringen und damit die Integrität und die Authentizität einer Datei sicherstellen. Das elektronische Siegel basiert in technischer Hinsicht auf den genau gleichen Verfahren wie die elektronische Signatur. Swisscom (Schweiz) AG erzeugt und verwaltet für den Siegelersteller treuhänderisch das Siegelzertifikat und stellt dieses für den Signing Service über einen verschlüsselten Kanal zur Verfügung. Somit benötigt der Siegelersteller für diesen Dienst ausser einer Teilnehmerapplikation keine weiteren Betriebsmittel, wie z.B. Token oder Signaturkarte.

Die Teilnehmerapplikation bereitet ein Dokument so auf, dass zur Siegelerstellung nur der Hash (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 Swisscom nicht ersichtlich. Der signierte Hash wird von der Teilnehmerapplikation wieder in das Dokument eingebaut und erzeugt damit ein signiertes Dokument. Alle über die gesicherte Schnittstelle vom Teilnehmer gesendeten Hashs der Dokumente werden von Swisscom signiert. Damit ist auch ein Batchbetrieb möglich. Der autorisierte Verbindungsaufbau wird hierbei vom Teilnehmer als Freigabe zur Siegelerstellung Swisscom gegenüber anerkannt. Der Teilnehmer kann die Teilnehmerapplikation auch für einen Siegelersteller als Dritten betreiben. Diesfalls benötigt Swisscom zur Siegelerstellung über die Teilnehmerapplikation des Teilnehmers eine Autorisierung des Siegelers.

Vor Aufnahme des Service stellt jeder Siegelersteller einen Zertifikatsantrag, der von Swisscom oder von einem Dritten unter der Verantwortung von Swisscom geprüft wird.



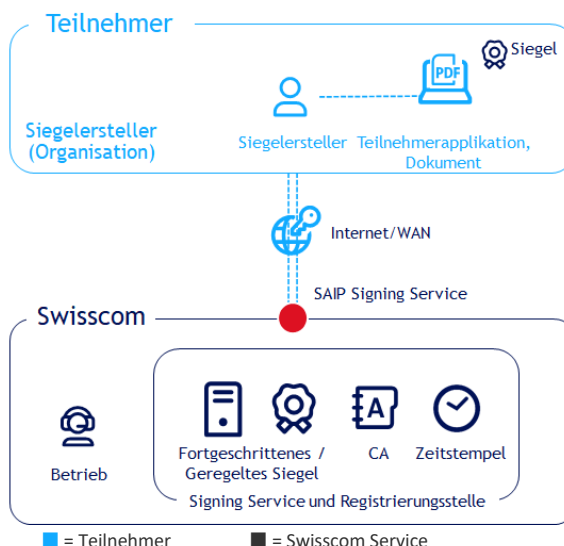


3 Definitionen

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 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

Ein Leistungsversprechen für das Funktionieren des Internets ist ausgeschlossen.

3.2 Servicespezifische Definitionen

| Begriff | Beschreibung |
|------------------------|---|
| CEN/TS 419 241 | CEN/DIN Norm für Fernsignaturen |
| CMS | Cryptographic Message Syntax – Eine im RFC5652 definierte Syntax für die digitale Signatur und kryptographische Mitteilungen. |
| CP/CPS | Zertifikatsrichtlinien (CP/CPS) der Swisscom (Schweiz) AG 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 Zertifikatssubjekt. Das Subjekt 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. |
| Elektronische Signatur | Die elektronische Signatur ist ein technisches Verfahren zur Überprüfung der Echtheit eines Dokuments, einer elektronischen Nachricht oder anderer elektronischer Daten sowie der Identität des Signierenden. |
| Elektronisches Siegel | Das elektronische Siegel basiert in technischer Hinsicht auf den genau gleichen Verfahren wie die elektronische Signatur. Elektronisches Siegel sind Daten in elektronischer Form, die anderen Daten in elektronischer Form beigelegt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen. |



| Begriff | Beschreibung |
|--|---|
| | Nach Schweizer Recht sind nur geregelte elektronische Siegel für UID-Einheiten gesetzlich geregelt, nicht hingegen fortgeschrittene elektronische Siegel. |
| FIPS 140-2 | Federal Information Processing Standard (Bundesstandard für Informationsverarbeitung), Bezeichnung für öffentlich bekanntgegebene Standards der USA |
| Hash | Eindeutige Abbildung einer grossen Datenmenge auf eine kleine Datenmenge, vergleichbar einem Fingerabdruck eines Dokumentes. Vom Hash können keinerlei Rückschlüsse auf den Dokumenteninhalt gezogen werden. |
| HSM | Hardware Security Module, deutsch: Hardware-Sicherheitsmodul, ein Peripheriegerät für die effiziente und sichere Ausführung von kryptographischen Funktionen und Applikationen, insbesondere auch zum Schutz der kryptographisch genutzten Schlüsselinformationen. |
| Nutzungsbestimmungen | Die Nutzungsbestimmungen regeln im Verhältnis zwischen Swisscom (Schweiz) AG und dem Siegelersteller auf einer Teilnehmerapplikation die Bedingungen für die Nutzung der Siegelzertifikate und Zertifizierungsdienstleistung. 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). |
| PKCS#1 | Kryptographischer Standard der RSA Laboratories. |
| RA | Registrierungsstelle (Registration Authority) |
| Registrierungsstelle (RA) | Zuständige Stelle für die Identifikation künftiger Siegelersteller. Kann vom Teilnehmer, Swisscom oder Dritten bereitgestellt werden unter der Voraussetzung eines Vertragsverhältnisses zur 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. |
| Signatur | Siehe "Elektronische Signatur" |
| Signaturzertifikat bzw. Siegelzertifikat | Zertifikat, welches auf den Signierenden bzw. den Siegelersteller ausgestellt ist, von Swisscom (Schweiz) AG treuhänderisch verwaltet wird und zur Signatur bzw. Siegelerstellung verwendet wird. |
| Signing Service | Der Signaturservice bietet eine Schnittstelle, die mit einer Teilnehmerapplikation zur Auslösung der Siegelerstellung verbunden wird. |
| Siegelersteller | Organisation (juristische Person, Verwaltungseinheiten etc.), die eine UID-Einheit ist im Sinne des Artikels 3 Absatz 1 Buchstabe c des schweizerischen Bundesgesetzes vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer (UIDG), in deren Namen ein digitales Zertifikat von Swisscom (Schweiz) AG ausgestellt wurde, auf Basis dessen sie ein fortgeschrittenes oder qualifiziertes elektronisches Siegel erstellt. Zukünftige Siegelersteller müssen bei Swisscom zunächst einen Antrag auf Ausstellen eines digitalen Zertifikats stellen. Bis zur Genehmigung des Antrags durch Swisscom sind Siegelersteller Antragsteller (die bei Ablehnung des Antrags keine Siegel erstellen können). |
| 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/TLS (Zugangs-) Zertifikaten. |
| Statische Signatur | Häufig in den technischen Unterlagen verwendeter Begriff für die "Organisationssignatur" oder "Siegel" gemäss dieser Leistungsbeschreibung. |
| 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 Reseller von Swisscom-Leistungen mit einer Annahmeerklärung gegenüber Swisscom (Schweiz) AG. Sofern der Teilnehmer nicht identisch mit dem Siegelersteller ist, benötigt der Teilnehmer eine Autorisierung dadurch, dass der Siegelersteller das Zugangszertifikat |



| Begriff | Beschreibung |
|-----------------------|---|
| | Swisscom elektronisch zusendet oder übergibt, oder das vom Teilnehmer autorisierte Zugangszertifikat Swisscom gegenüber akzeptiert. |
| Teilnehmerapplikation | Der Teilnehmer gibt einem oder mehreren Siegelersteller Zugang zu einer Applikation, mit der er oder sie elektronische Siegel gemäss den Nutzungsbestimmungen von Swisscom (Schweiz) AG erstellen können und der Teilnehmer stellt dabei neben der Authentisierung die Übertragung der Siegeldaten zum Fernsignaturservice von Swisscom sicher. Die Teilnehmerapplikation nimmt die signierten Daten entgegen und bereitet für den Siegelersteller das Dokument auf. Die Teilnehmerapplikation ist nicht Bestandteil dieser Leistungsbeschreibung, sie wird ausserhalb des Signing Service- Service z.B. durch Partner von Swisscom bereitgestellt. |
| UID-Einheit | Organisation gemäss Art. 3 Abs. 1 Bst. c UIDG, der eine Unternehmens-Identifikationsnummer (UID) zur eindeutigen Identifizierung zugeordnet wurde. Nur UID-Einheiten können Ersteller für elektronische Siegel gemäss CP/CPS sein. |
| UIDG | Schweizerisches Bundesgesetz vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer |
| ZertES | Schweizerisches Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate |
| Zugangszertifikat | Zertifikat, welches einerseits den Zugang der Teilnehmerapplikation zum Signing Service authentisiert und andererseits zur verschlüsselten Kommunikation mit dem Signing Service dient. Es handelt sich um ein öffentlich vertrauenswürdigen oder vom Teilnehmer selbst signiertes SSL/TLS-Zertifikat, welches auch den öffentlichen Schlüssel enthält. Die Spezifikation ist in der Konfigurations- und Annahmeerklärung enthalten. Falls Teilnehmer und Siegelersteller identisch sind, stellt ein bevollmächtigter Vertreter des Teilnehmers das Zugangszertifikat Swisscom elektronisch zu (z.B. per E-Mail). Falls Teilnehmer und Siegelersteller nicht identisch sind, braucht es zusätzlich zur Übergabe des Zugangszertifikats an Swisscom auch eine schriftliche Genehmigung des Siegelers, welche die Verwendung des Zugangszertifikats zur Erstellung elektronischer Siegel im Namen des Siegelers über die Teilnehmerapplikation des Teilnehmers gegenüber Swisscom (Schweiz) AG zulässt. Im Falle eines geregelten Zertifikates behält der Siegelersteller immer den Zugriff auf den privaten Schlüssel dieses Zugangszertifikates und übergibt dieses persönlich an Swisscom. |

4 Ausprägungen und Optionen

| Standardausprägung | Elektronische Siegel |
|--|----------------------|
| Fortgeschrittenes elektronisches Siegel | ● |
| Geregeltes elektronisches Siegel | ● |
| Qualifizierter elektronischer Zeitstempel | ● |
| Datenaufbewahrung in der Schweiz | ● |
| Betrieb gem. Zertifikatsrichtlinien (CP/CPS) | ● |
| Behördensiegel | ○ |

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

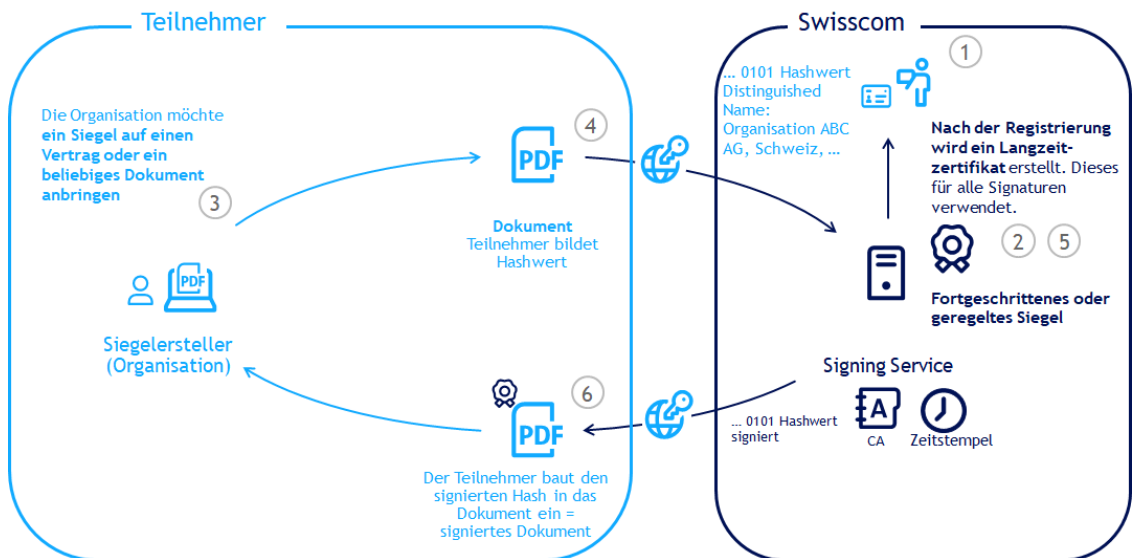
4.1 Definition der Leistungen

| Leistung | Definition |
|---|--|
| Fortgeschrittenes elektronisches Siegel | Fortgeschrittenes elektronisches Siegel gemäss ETSI Standard 319 411 "NCP+" |
| Geregeltes elektronisches Siegel | Geregeltes elektronische Siegel gemäss Art. 2 Bst. d ZertES: eine fortgeschrittene elektronische Signatur, die unter Verwendung einer sicheren Siegelerstellungseinheit nach Artikel 6 ZertES erstellt wurde und auf einem geregelten und zum Zeitpunkt der Erzeugung des elektronischen Siegels gültigen Zertifikat beruht. Die Siegelzertifikate können ausschliesslich im Namen einer UID-Einheit ausgestellt werden. |



| Leistung | Definition |
|--|---|
| Qualifizierter elektronischer Zeitstempel | Qualifizierter elektronischer Zeitstempel gemäss Art. 2 Bst. j ZertES. |
| Datenaufbewahrung in der Schweiz | Die Datenaufbewahrung mit den Personendaten aus den Zertifikaten findet nur in der Schweiz im Einklang mit den einschlägigen Vorschriften der schweizerischen Datenschutzgesetzgebung statt. |
| Betrieb gem. Zertifikatsrichtlinien (CP/CPS) | <p>Der Betrieb eines Zertifizierungsdienstanbieters richtet sich nach den Zertifikatsrichtlinien (CP/CPS) der Swisscom (Schweiz) AG zur Ausstellung von Siegelzertifikaten.</p> <p>Diese können in der aktuellsten Fassung hier aufgerufen werden: https://trustservices.swisscom.com/repository/ Geregelte elektronische Siegel basieren auf geregelten Zertifikaten (Klasse „Diamant“). Fortgeschrittene Siegel basieren auf Zertifikaten der Klasse "Saphir".</p> |
| Behördensiegel | Behördensiegel sind geregelte Siegelzertifikate, die gemäss den "Technisch Administrativen Vorschriften" (TAV) zum ZertES vom 15.3.2022 für Behörden ausgestellt werden. Diese werden von Swisscom mit den in Kapitel 2.3.4 a) der TAV spezifizierten Vorschriften zu den Behördenbezeichnungen in den OU Feldern ausgestellt, allerdings ohne das optionale Feld businessCategorie gemäss 2.3.4 b) der TAV. |

4.2 Ablauf der Siegelerstellung



- Die Registrierungsstelle (1) prüft den Siegelersteller vorab anhand von Registereinträgen und nimmt einen Antrag eines berechtigten Vertreters des Siegelers entgegen. Dieser muss vor einem von Swisscom ernannten Berechtigten persönlich erscheinen (z.B. Identifikation mit RA-App). Der Antrag und weitere eingereichte Unterlagen werden geprüft und archiviert.
- Nach Genehmigung des Antrags wird für den Siegelersteller das Schlüsselmateriale auf der Signing Service Plattform erzeugt und hinterlegt (2). Zu diesem Schlüsselpaar wird ein entsprechendes Langzeit-Siegelzertifikat (in der Regel 3 Jahre) gemäss den Zertifikatsrichtlinien der Swisscom (Schweiz) AG und dem im Siegelzertifikatsantrag benannten Subjekt des Siegelzertifikates (Distinguished Name des Siegelers) ausgestellt.
- Der vom Siegelersteller autorisierte Teilnehmer oder der Siegelersteller selbst erstellt ein SSL/TLS Zugangszertifikat. Der Teilnehmer hinterlegt es auf seinem Server. Ausserdem lässt der Teilnehmer eine Kopie dieses Zugangszertifikates der Swisscom zukommen, die es auf der Signing Service Plattform hinterlegt. So wird die Verbindung zwischen der Teilnehmerapplikation und dem Signing Service abgesichert.
- Bei Ausstellung eines geregelten Siegels muss die Registrierung und Nutzung der Authentisierungsmittel mit einem vom Antragssteller beschriebenen Verfahren durchgeführt werden, das von Swisscom zugelassen ist und der in [CEN/TS 419 241] beschriebenen Stufe 2 (Sole Control Assurance Level 2) entspricht. Z.B. könnte der private Schlüssel des Zugangszertifikates auf einem mit Swisscom oder seinem Partner vereinbarten, kryptographischen Modul oder erzeugt und verwaltet werden. Die Erstellung des privaten Schlüssels geschieht in diesem Beispiel beim Teilnehmer, wo das kryptographische Modul oder das HSM liegt, in Anwesenheit eines von Swisscom ernannten Berechtigten.



- Mit diesem Zugangszertifikat werden zudem alle Signaturaufträge authentisiert, eine weitere Einzelauthentisierung findet nicht mehr statt.
- Der Siegelersteller wählt das zu signierende Dokument (3) oder einen Stapel von Dokumenten aus. Die Teilnehmerapplikation bildet einen Hash nach Vorgaben von Swisscom (4) und sendet ihn an den Signing Service. Weiterhin werden auch für das Siegelzertifikatsubject relevante Angaben (Distinguished Name) von der Teilnehmerapplikation übergeben.
- Sofern der Distinguished Name des Siegelerstellers von der Registrierungsstelle erfasst und für die Siegelerstellung zugelassen ist, erfolgt eine Signatur des Hashs (5) nach CMS oder PKCS#1 Standard, um dessen Integrität sicher zu stellen.
- Das Siegel mit zusätzlichen Validierungsinformationen im Signaturzertifikat (z.B. Signaturzertifikatskette zum vertrauenswürdigen Root-Zertifikat sowie qualifizierter Zeitstempel) wird zurückgegeben. Die Teilnehmerapplikation stellt das Siegel des Dokumentes durch Einbettung des signierten Hashs in das Dokument sicher. (6)
- Die Sicherheit der Teilnehmerapplikation wird durch regelmässige Selbstaudits des Teilnehmers gemäss der Konfigurations- und Annahmeerklärung sowie bei Bedarf durch ein Audit durch Swisscom sichergestellt.

4.3 Prozess zur Prüfung eines Siegelerstellers

Vor der Aufschaltung des Service führt Swisscom eine Prüfung des Siegelerstellers gemäss den Bestimmungen der CP/CPS (siehe oben) durch. Hierzu muss der Siegelersteller im Siegelzertifikatsantrag benannt sein und ein zeichnungsberechtigter Vertreter des Siegelerstellers muss den Antrag für ein Siegelzertifikat unterzeichnet haben. Im Falle von Unterschriftenregelungen durch zwei Zeichnungsberechtigte muss noch ein weiterer Vertreter des Siegelerstellers mitunterzeichnen. Mit der Unterzeichnung des Siegelzertifikatsantrages ermächtigt der Siegelersteller Swisscom zur Ausstellung des Zertifikates. Die Unterschriften müssen entweder qualifiziert elektronisch oder handschriftlich in persönlicher Anwesenheit eines von Swisscom befugten Vertreters erfolgen.

4.4 Revokation (Ungültigkeitserklärung) eines Siegelzertifikates

Siegelzertifikate und/oder Zugangszertifikate müssen vom Siegelersteller als ungültig erklärt werden, sofern Anzeichen eines Missbrauches oder Kompromittierung sichtbar werden. Swisscom stellt danach ein neues Siegelzertifikat aus, ggfs. auch auf Basis eines neuen Zugangszertifikates.

Eine Meldung zur Revokation hat durch die im Zertifikatsantrag benannte Vertreterin des Siegelerstellers zu erfolgen, deren Authentifizierungsmittel (Mobilnummer) bei Swisscom hinterlegt wurde. Diese kann online unter

<https://trustservices.swisscom.com/repository/> erfolgen. Ein Revokationsantrag wird mittels der hinterlegten Mobilnummer bzw. der für die persönliche Signatur des Antrages verwendeten Authentisierungsmethode überprüft. Weitere Verfahren zur Revokation sind gemäss Bestimmungen der CP/CPS möglich.

5 Leistungsdarstellung und Verantwortlichkeiten

Einmalige Leistungen

| Tätigkeiten (S = STS/T = Teilnehmer) | S | T |
|--------------------------------------|---|---|
| Bereitstellung des Service | | |



| Tätigkeiten (S = STS/T = Teilnehmer) | | S | T |
|--|---|---|---|
| 1. | Bereitstellung der Signing Service Infrastruktur. | ✓ | |
| 2. | Bereitstellung der Schnittstelle SAIP basierend auf OASIS DSS Protokoll über SOAP oder REST. 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. | ✓ | |
| 3. | 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 2. | | ✓ |
| 4. | Zusenden der unterzeichneten Annahmeerklärung mit aktivierungsrelevanten Informationen und den geforderten Ansprechpartnern | | ✓ |
| 5. | Umsetzung der Auflagen der Annahmeerklärung | | ✓ |
| 6. | Bereitstellung eines vom Siegelsteller unterzeichneten Antrages zum Siegelzertifikat mit allen notwendigen Dokumenten zur Überprüfung des Siegelstellers (z.B. beglaubigter Handelsregistrauszug bei geregelter Siegel) sowie der Zustimmung zu den Nutzungsbestimmungen des Service. Unterschrift im Antrag zum Siegelzertifikat durch einen für den Siegelsteller zeichnungsberechtigten Vertreter. Veranlassung der Identifikation durch persönliches Erscheinen eines Vertreters des Siegelstellers oder durch qualifizierte elektronische Signatur. Der Teilnehmer stellt sicher, dass der OU Eintrag (Organizational Unit) im Siegelantrag namensrechtlich nicht mit einer anderen Organisation kollidiert. | | ✓ |
| 7. | Sicherstellung der Zusendung eines Zugangszertifikates an Swisscom durch den Siegelsteller oder dessen Bevollmächtigten mit Bestätigung der Vollmacht. | | ✓ |
| 8. | Sofern geregelte elektronische Siegel erstellt werden muss ein von Swisscom freigegebenes Verfahren zur Authentisierung und Willensbekundung befolgt werden. Swisscom wird mit dedizierten Partnern ein Verfahren freigeben. | | ✓ |
| 9. | Freischaltung der Kommunikation für das zugesendete Zugangszertifikat. | ✓ | |
| 10. | Ggfs. Konfiguration der Firewall, serverseitig beim Teilnehmer. | | ✓ |
| 11. | Benennung eines Verantwortlichen inklusive laufender Stellvertretung für alle Fragen bezüglich der Technik und Sicherheit und Ansprechpartner für Auditfragen in der Konfigurations- und Annahmeerklärung. | | ✓ |
| 12. | Prüfung der Antragsunterlagen. | ✓ | |
| 13. | Aufschalten des Teilnehmers und Zusenden der teilnehmerspezifischen Zugangsdaten. | ✓ | |
| 14. | Einbindung des Signing Services in die teilnehmerspezifische Anwendung(en) bzw. teilnehmerseitige Anbindung der Schnittstelle zum Signing Service, z.B. durch Einsatz einer Teilnehmerapplikation eines Partners. | | ✓ |
| 15. | Prüfung des Zugriffs auf den Signing Service und der Angaben auf dem Siegelzertifikat. Umgehende Meldung allfälliger Fehler an Swisscom, bevor dieses für eine Siegelerstellung benutzt wird. | | ✓ |
| 16. | Fehlerbehebung durch Update oder Neuinstallation. | ✓ | |
| 17. | Betrieb einer Revokationsstelle zur Ungültigkeitserklärung eines Siegelzertifikates bei Kompromittierung oder aus anderen Gründen | ✓ | |
| 18. | Revozieren und Ermöglichung von Revokationen durch den Siegelsteller bei Anzeichen einer Kompromittierung vom Siegel- oder Zugangszertifikat über ein von Swisscom publiziertes Revokationsverfahren. | | ✓ |
| 19. | Meldung der Aufgabe der Geschäftstätigkeit sowie eine gegen den Teilnehmer gerichtete Konkursandrohung, die erfolgte Konkursöffnung oder eine Nachlassstundung. | | ✓ |
| Beendigung des Service oder Beendigung der Siegelerstellung für einen Siegelsteller | | | |
| 1. | Löschen der Siegel- und Zugangszertifikate in der Signing Service Infrastruktur. | ✓ | |
| 2. | Löschen der zugehörigen Schlüssel aus dem HSM. | ✓ | |

Wiederkehrende Leistungen



| Tätigkeiten (S = STS/T = Teilnehmer) | | S | T |
|--------------------------------------|--|---|---|
| Standardleistungen | | | |
| 1. | Betrieb der Signing Service Infrastruktur, Erneuerung des Siegelzertifikates rechtzeitig vor Ablauf der Gültigkeit. | ✓ | |
| 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 usw.). Offenlegung des Sicherheitsdispositivs der Teilnehmerapplikation und der Kommunikation zu Swisscom, sofern von Swisscom oder dessen Anerkennungsstelle verlangt. | | ✓ |
| 5. | Anpassung der Definition der Sicherheitsanforderungen. | ✓ | |
| 6. | Lifecycle-Management des Zugangszertifikates: rechtzeitiger Austausch vor Ablauf der Gültigkeit durch den Siegelersteller selber mittels E-Mail an den 1st Level Support der Swisscom unter Bezeichnung der Claimed Identity und der im Vertrag genannten PRO Nummer. | | ✓ |
| 7. | Sicherstellung der Vertraulichkeit des Datenaustauschs zwischen Swisscom und dem Teilnehmer (z.B. Vermeidung von "Inspection" Modulen). | | ✓ |
| 8. | Sofern geregelte elektronische Siegel erstellt werden: Auswahl eines kryptographischen Moduls oder HSM, das den Zugriff auf die Teilnehmerapplikation spätestens nach 5 Fehlversuchen zur Authentisierung am Service sperrt. Es muss nach einer Sperrung ein neues Zugangszertifikat in einer gemeinsamen Zeremonie mit Swisscom erstellt werden. | | ✓ |
| 9. | Erstellung von Siegelzertifikaten | ✓ | |
| 10. | Festlegung der Siegelzertifikatsinhalte und Verfahren zur Siegelerstellung. | ✓ | |
| 11. | Übermittlung der Daten des Siegelerstellers (Distinguished Name) gemäss den Vorgaben im Zertifikatsantrag des Siegelerstellers und in der Konfigurations- und Annahmeerklärung. | | ✓ |
| 12. | Durchführen von Siegelerstellungen. | ✓ | |
| 13. | Durchführung der Siegelerstellung in Verbindung mit einem qualifizierten Zeitstempel nach ZertES. | ✓ | |
| 14. | Sicherstellen der Mitwirkungsleistungen und Auflagen durch den Sicherheitsverantwortlichen. | | ✓ |
| 15. | Teilnehmerinformation bei Störungen und Wartungen. | ✓ | |
| 16. | Bereitstellung der Supportdienstleistungen (Service Desk, Incident Management usw.) | ✓ | |
| 17. | Melden von Mutationen der teilnehmerspezifischen Informationen (Kontaktpersonen, Zugangszertifikat, Beendigung der Siegelerstellung usw.) | | ✓ |
| 18. | Nachführen der teilnehmerspezifischen Informationen (Kontaktpersonen, Zugangszertifikat usw.) | ✓ | |
| 19. | Meldung von Service Störungen | ✓ | |
| 20. | Melden von Sicherheitsvorfällen auf dem System der Teilnehmerapplikation, die den Signing Service betrifft. | | ✓ |
| 21. | Melden von Sicherheitsvorfällen auf dem System des Signaturservice, die Auswirkung auf den Teilnehmer oder Siegelersteller hat | ✓ | |
| 22. | 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. | ✓ | |
| 23. | Anpassung der Schnittstelle an die neuen Vorgaben von Swisscom binnen von 3 Monaten. | | ✓ |

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 (Monitored Operation Time, Support Time, Availability, Security und Continuity) sowie die Beschreibung des Messverfahrens und des Reportings ergeben sich aus dem Vertragsbestandteil Basisdokument (z.B. "SLA-Definitionen"). Folgende Service Levels werden erbracht. Bei mehreren möglichen Service Levels pro Ausprägung erfolgt die Auswahl des Service Levels im Servicevertrag.



| Service Level & Zielwerte | | | Elektronische Siegel |
|--|--|--|----------------------|
| 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% | | ● |
| • Verzeichnis-Dienste nach CP/CPS Ziffer 2.2 | 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 Rechnungsstellung erfolgt jeweils rückwirkend für den vergangenen Monat. Die Details zur Rechnungsstellung werden im Service Vertrag geregelt.

7.2 Mengenreport

Mengenreports werden im Service Vertrag 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.



8 Besondere Regelungen

8.1 Teilnehmerapplikation

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

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

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

8.3 Einsatzmöglichkeiten des fortgeschrittenen oder geregelten elektronischen Siegels

Die Verwendung des fortgeschrittenen oder geregelten elektronischen Siegels dient in der Regel dazu, den Herkunftsnachweis sowie die Integrität des Inhalts einer Datei zu gewährleisten. Das elektronische Siegel ist nicht mit dem rechtlichen Konzept der elektronischen Signatur zu verwechseln. Zudem sind die Rechtswirkungen des höherwertigen geregelten elektronischen Siegels nicht dieselben wie diejenigen des fortgeschrittenen elektronischen Siegels. Es obliegt dem Teilnehmer und seinen Siegelersteller, die Rechtswirkungen der gewählten Art der elektronischen Siegel (mit und ohne Zeitstempel) im Voraus abzuklären. Swisscom übernimmt hierfür keine Verantwortung.

Geregeltes elektronisches Siegel (auf der Basis eines Zertifikats der Swisscom (Schweiz) AG-Klasse Diamant): Das über den Signing Service erstellte geregelte Siegel erfüllt die in der CP/CPS definierten Eigenschaften und die Definition gemäss Art. 2 Bst. d des Schweizer Bundesgesetzes über die elektronische Signatur (ZertES; SR 943.03).

Fortgeschrittenes elektronisches Siegel (Zertifikat der Swisscom (Schweiz) AG-Klasse Saphir): Das über den Signing Service erstellte fortgeschrittene elektronische Siegel erfüllt die in der CP/CPS definierten Eigenschaften und ist im Unterschied zum geregelten elektronischen Siegel nicht gesetzlich geregelt.

Qualifizierter elektronischer Zeitstempel: Der über den Signing Service erstellte qualifizierte elektronische Zeitstempel erfüllt die in der CP / CPS definierten Eigenschaften und die Definition gemäss Art. 2 Bst. j ZertES.

Weder das fortgeschrittene elektronische Siegel noch das geregelte elektronische Siegel haben die gleichen Rechtswirkungen wie eine handschriftliche Unterschrift oder eine qualifizierte elektronische Signatur. Je nach Situation benötigen gewisse Dokumente also die handschriftliche Unterschrift, eine qualifizierte elektronische Signatur oder ein geregeltes elektronisches Siegel ggfs. mit einem elektronischen Zeitstempel, damit beabsichtigte Rechtswirkungen überhaupt eintreten können.

Über den Signing Service ausgestellte elektronische Siegel können bei Anwendbarkeit ausländischen Rechts abweichende, allenfalls weitergehende oder weniger weitgehende Wirkungen entfalten als dies nach Schweizer Recht der Fall ist.

Der Austausch verschlüsselter Daten und die Ausstellung von Zertifikaten unterliegt zudem in/mit gewissen Staaten gesetzlichen Restriktionen.

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

Die im Rahmen der Leistungserbringung vom Teilnehmer an Swisscom übermittelten Daten (Siegelerstellerdaten) werden grundsätzlich von Swisscom in der Schweiz bearbeitet. Eine Datenbearbeitung durch von Swisscom 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 temporär VPN-Zugriff auf das Netzwerk von Swisscom mit Applikationsdaten, die keine Personendaten beinhalten. Dabei können in Einzelfällen auch die vom Siegelersteller im Zertifikat veröffentlichten Signaturdaten und Stammdaten des Siegelers (z.B. Organisationsname, Bezeichnung des vom Teilnehmer veröffentlichten Zugangszertifikates) 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.