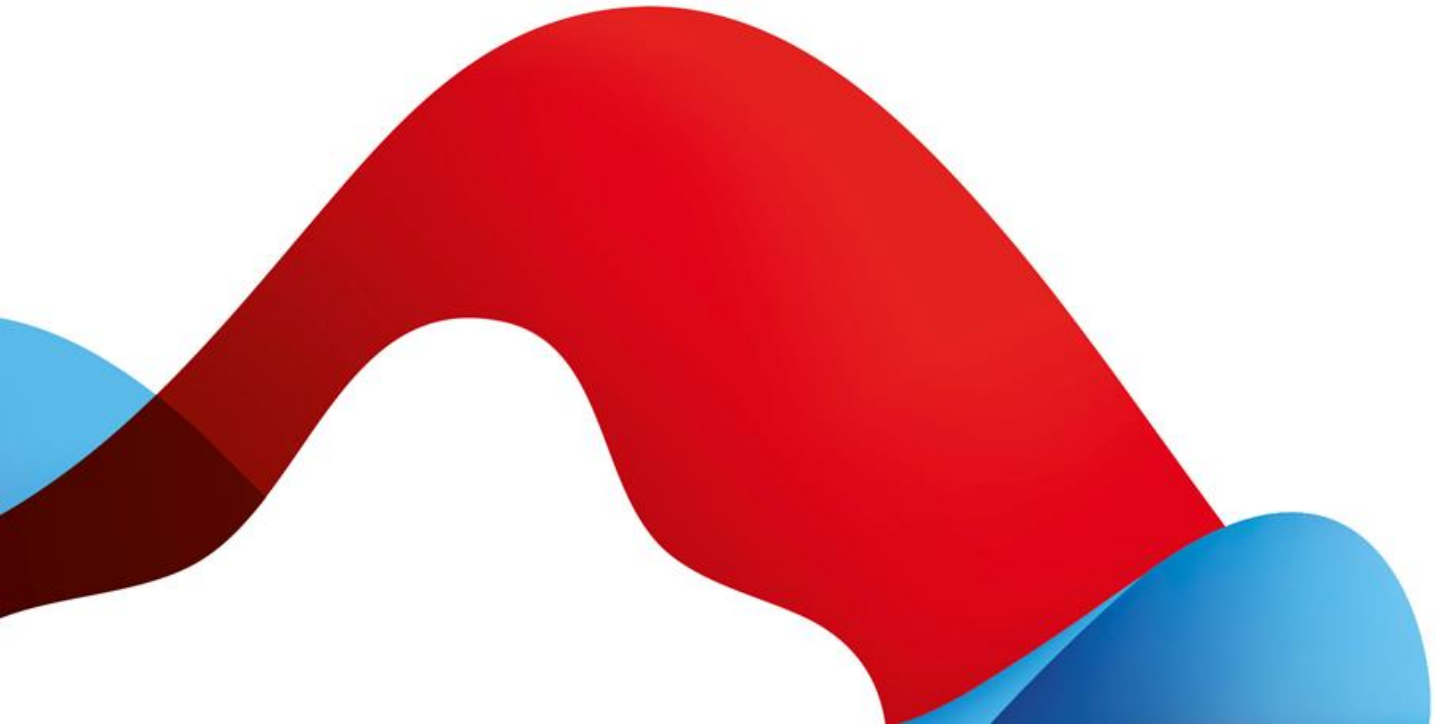
Leistungsbeschreibung

All-in Signing Service für EU Siegel (Static Signaturen)



Inhaltsverzeichnis

1 Übersicht zum Service

Der All-in Signing Service (AIS) ist eine serverbasierte Fernsignaturdienstleistung der Swisscom IT Services Finance S.E., Wien (AT), nachfolgend Swisscom "ITSF" genannt. Der All-in Signing (AIS) Service wird in den Rechenzentren von Swisscom (Schweiz) AG in der Schweiz bereitgestellt und Swisscom (Schweiz) AG vertreibt den AIS Service in eigenen Namen oder räumt Dritten wiederum das Recht ein, den AIS Service in eigenem Namen zu vertreiben.

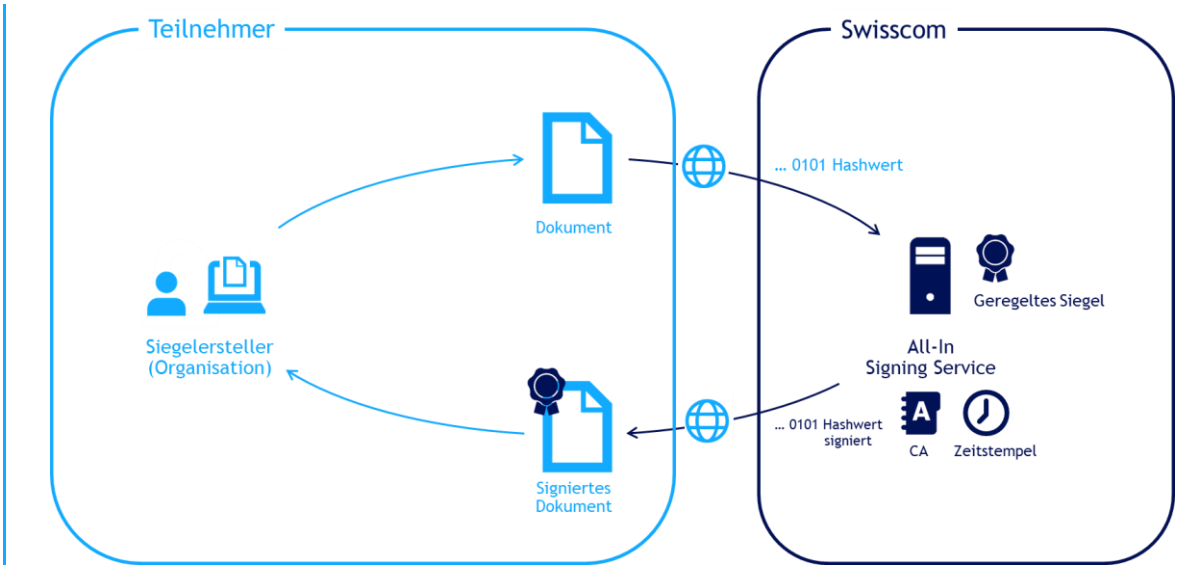
Swisscom ITSF ist in der EU für die Ausstellung elektronischer Siegel qualifizierte Vertrauensdiensteanbieterin gemäss eIDAS-Verordnung und österreichischem Signatur- und Vertrauensdienstegesetz (SVG). Eine Konformitätsbewertungsstelle prüft regelmässig, ob die Anforderungen, die das europäische und österreichische Recht und / oder technische Normen an eine anerkannte Anbieterin von Zertifizierungsdiensten im Bereich der elektronischen Signatur stellt, auch erfüllt werden. Die Aufsichtsstelle hat Swisscom ITSF den Qualifikationsstatus als qualifizierte Vertrauensdiensteanbieterin für die Ausstellung qualifizierter Zertifikate für elektronische Signaturen und elektronische Siegel verliehen. Swisscom ITSF ist auf den Vertrauenslisten gemäss Art. 22 eIDAS-Verordnung aufgenommen und berechtigt, das EU-Vertrauenssiegel zu verwenden.

Allgemein bietet Swisscom ITSF je nach konkreter Vertragsgestaltung fortgeschrittene und qualifizierte elektronische Signaturen für natürliche Personen sowie fortgeschrittene und qualifizierte elektronische Siegel für Organisationen an. Vorliegende Leistungsbeschreibung beschreibt den Service für fortgeschrittene und qualifizierte elektronische Siegel für juristische Personen im Sinne der Gesetzgebung der EU (eIDAS-Verordnung).

Siegelerstellende Organisationen (nachfolgend "Siegelersteller", vgl. hierzu die detaillierte Definition unter Ziffer 2) können mit AIS 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. Der Vertrauensdienst von Swisscom ITSF erzeugt und verwaltet unter Beizug von Swisscom (Schweiz) AG für den Siegelersteller treuhänderisch das Siegelzertifikat und stellt dieses für den AIS 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-Wert (Prüfsumme fester Länge ohne Rückschluss auf den Inhalt) an den AIS 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 und vom Siegelersteller authentisierte Schnittstelle gesendeten Dokumentenhashwerte werden von Swisscom ITSF signiert. Damit ist auch ein Batchbetrieb möglich. Der autorisierte Verbindungsaufbau wird hierbei als Freigabe zum Siegel 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 Siegelerstellers.

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

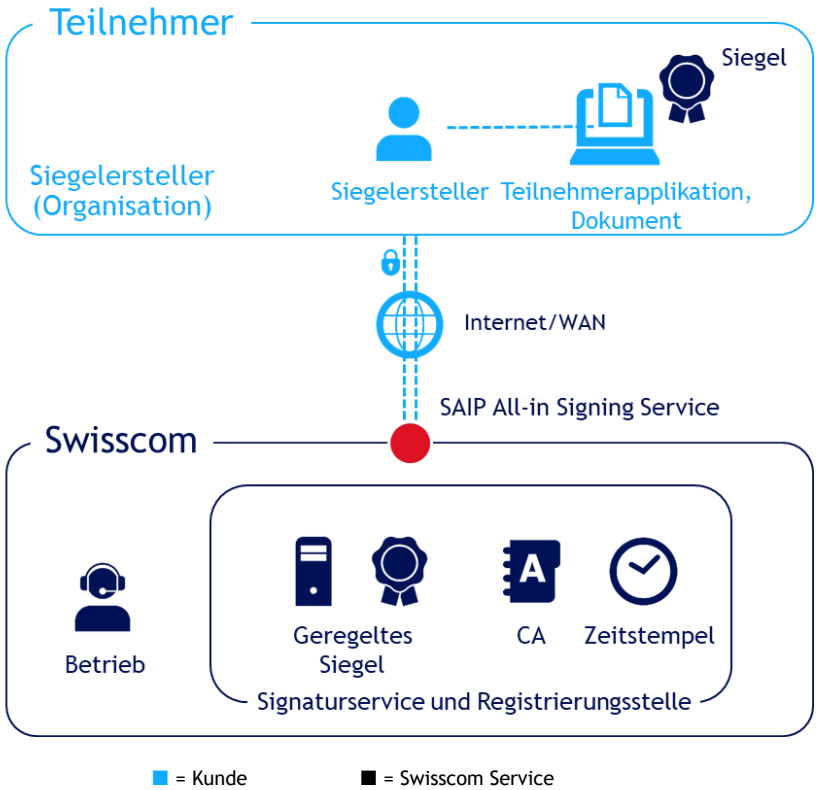


2 Definitionen

2.1 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 All-in Signing Service:



2.2 Servicespezifische Definitionen

Begriff	Beschreibung
AIS	All-In Signing
AIS Service	All-In Signing Service. Der Signaturservice bietet eine Schnittstelle, die mit einer Teilnehmerapplikation zur Auslösung der Siegelerstellung verbunden wird.
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.
eIDAS-Verordnung / eIDAS-VO	Verordnung Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG; regelt insbesondere auch die elektronische Signatur.
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 beigefügt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen. Diese Leistungsbeschreibung beschreibt die durch die eIDAS-VO definierten fortgeschrittenen und qualifizierten elektronischen Siegel.
ETSI Standard 319 411	European Telecommunications Standards Institute (ETSI) publiziert Standards für verschiedene Bereiche in der Informations- und Kommunikationstechnologie. Für die digitale Signatur ist u.a. der Standard 319 411 massgeblich, der Anforderung an verschiedene Level der Vertrauenswürdigkeit von Signaturen definiert.
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 IT Finance Service S.E. und dem Siegelersteller auf einer Teilnehmerapplikation die Bedingungen für die Nutzung der Siegelzertifikate und Zertifizierungsdienstleistung. Diese sind unter https://www.swissdigicert.ch abrufbar.

Begriff	Beschreibung
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 (**R**egistration **A**uthority)
Registrierungsstelle (RA)	Zuständige Stelle für die Identifikation künftiger Siegelersteller. Kann vom Teilnehmer, Swisscom oder Dritten bereitgestellt werden unter der Voraussetzung eines Vertragsverhältnisses zu Swisscom.
REST	Representational State Transfer, Programmierparadigma für verteilte Systeme, insbesondere Webservices.
Sichere Signatur-Erstellungseinheit (HSM)	Qualifizierte und zertifizierte Hardware zur Erstellung von Signaturschlüsseln und Signaturzertifikaten.
Siegelersteller	Juristische Person im Sinne der eIDAS-VO, in deren Namen ein digitales Zertifikat von Swisscom ausgestellt wurde, auf Basis dessen sie ein fortgeschrittenes oder qualifiziertes 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 digitalen Siegel erstellen können).
Signatur	Siehe "Elektronische Signatur"
Signaturzertifikat bzw. Siegelzertifikat	Zertifikat, welches auf den Signierenden bzw. den Siegelersteller ausgestellt ist, von Swisscom treuhänderisch verwaltet wird und zur Signatur bzw. Siegelerstellung verwendet wird.
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 einen All-in Signing Service Vertrag (inklusive Konfigurations- und Annahmeerklärung) oder er hat einen kommerziellen Vertrag mit einem Partner von Swisscom mit einer Konfigurations- und Annahmeerklärung gegenüber Swisscom. Sofern der Teilnehmer nicht identisch mit dem Siegelersteller ist, benötigt der Teilnehmer eine Autorisierung dadurch, dass der Siegelersteller das Zugangszertifikat Swisscom elektronisch zusendet oder übergibt oder das vom Teilnehmer autorisierte Zugangszertifikat Swisscom gegenüber akzeptiert.
Teilnehmerapplikation	Der Teilnehmer gibt einem oder mehreren Siegelerstellern Zugang zu einer Applikation, mit der er oder sie fortgeschrittene elektronische Siegel oder qualifizierte elektronische Siegel gemäss den Nutzungsbestimmungen von Swisscom 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 AIS z.B. durch Partner von Swisscom bereitgestellt.

Begriff	Beschreibung
Zugangszertifikat	Zertifikat, welches einerseits den Zugang der Teilnehmerapplikation zum AIS authentisiert und andererseits zur verschlüsselten Kommunikation mit dem AIS Service dient. Es handelt sich um ein öffentlich vertrauenswürdiges 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 Siegelerstellers, welche die Verwendung des Zugangszertifikats zur Erstellung von elektronischen Siegel im Namen des Siegelerstellers mit der Teilnehmerapplikation des Teilnehmers gegenüber Swisscom zulässt. Im Falle eines qualifizierten Zertifikates behält der Siegelersteller immer den Zugriff auf den privaten Schlüssel dieses Zugangszertifikates und übergibt dieses persönlich an Swisscom.

3 Ausprägungen und Optionen

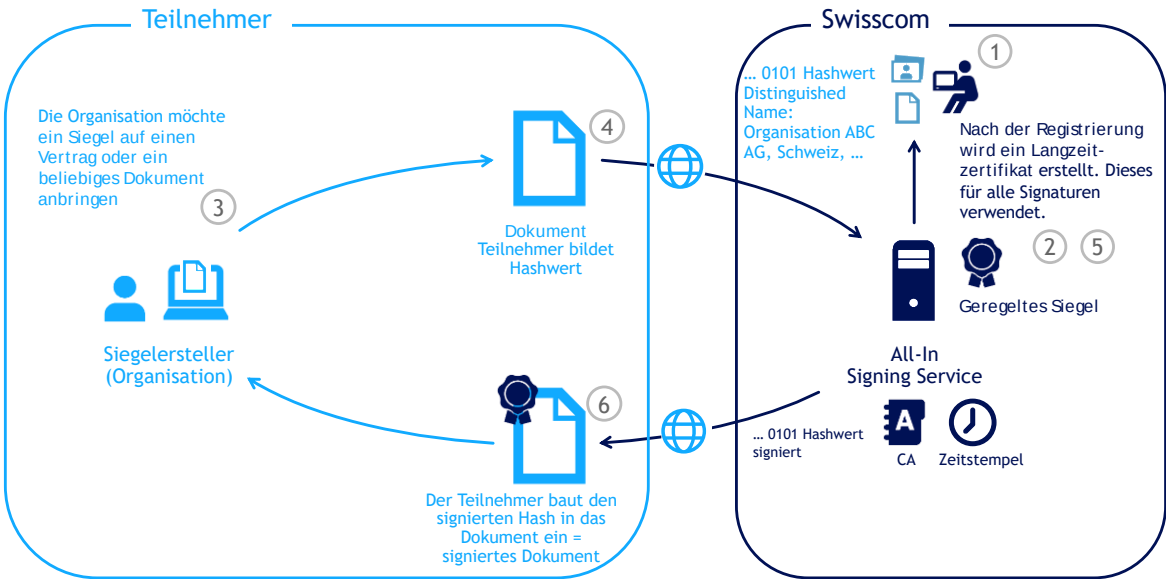
Standardausprägung	Elektronische Siegel
Fortgeschrittenes elektronisches Siegel	●
Qualifiziertes elektronisches Siegel	●
Elektronischer Zeitstempel	●
Datenaufbewahrung in der Schweiz	●
Betrieb gem. Zertifikatsrichtlinien (CP/CPS)	●

● = Standard (im Preis inbegriffen)

3.1 Definition der Leistungen

Leistung	Definition
Fortgeschrittenes elektronisches Siegel	Fortgeschrittenes elektronisches Siegel gemäss Art. 3 Ziff. 26 eIDAS-VO und gemäss ETSI Standard 319 411 "NCP+"
Qualifiziertes elektronisches Siegel	Qualifiziertes elektronisches Siegel gemäss Art. 3 Ziff. 27 eIDAS-VO. Dieses kann ausschliesslich im Namen einer juristischen Person im Sinn der eIDAS-VO ausgestellt werden.
Elektronischer Zeitstempel	Elektronischer Zeitstempel im Sinn von Art. 3 Ziff. 33 eIDAS-VO, der nicht die Anforderungen des qualifizierten Zeitstempels nach Art. 3 Ziff. 34 eIDAS-VO erfüllt.
Datenaufbewahrung in der Schweiz	Die Aufbewahrung der Personendaten aus den Zertifikaten findet in der Schweiz statt, im Einklang mit den einschlägigen Vorschriften der EU-DSGVO und der schweizerischen Datenschutzgesetzgebung.
Betrieb gem. Zertifikatsrichtlinien (CP/CPS)	Der Betrieb eines Vertrauensdiensteanbieters richtet sich nach den Zertifikatsrichtlinien der Swisscom ITSF (CP/CPS) zur Ausstellung von Signaturzertifikaten. Diese können in der aktuellsten Fassung hier aufgerufen werden: http://www.swissdigicert.ch/download_docs (Spalte EU) Fortgeschrittene elektronische Siegel basieren auf Zertifikaten der Klasse „Saphir“ und qualifizierte elektronische Siegel basieren auf Zertifikaten der Klasse "Diamant".

3.2 Ablauf der Siegelerstellung für alle Optionen



- Die Registrierungsstelle (1) prüft den Siegelersteller vorab anhand von Registereinträgen und nimmt einen Antrag eines befugten Vertreters des Siegelerstellers entgegen. Dieser muss bei qualifizierten Siegeln vor einem von Swisscom ernannten Berechtigten persönlich erscheinen. Der Antrag und weitere eingereichte Unterlagen werden geprüft und archiviert.
- Nach Genehmigung des Antrags wird für den Siegelersteller das Schlüsselmaterial auf der AIS Plattform erzeugt und hinterlegt (2). Zu diesem Schlüsselpaar wird ein entsprechendes Langzeit-Siegelzertifikat (in der Regel 3 Jahre) gemäss den Zertifikatsrichtlinien der Swisscom und dem im Siegelzertifikatsantrag benannten Subjekt des Siegelzertifikates (Distinguished Name des Siegelerstellers) 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 AIS Plattform hinterlegt. So wird die Verbindung zwischen der Teilnehmerapplikation und dem AIS Service abgesichert.
- Im Falle von qualifizierten Siegeln muss der private Schlüssel des Zugangszertifikates auf einem mit Swisscom oder seinem Partner vereinbarten, kryptographischem Modul oder HSM mit Mindeststandard FIPS 140-2 erzeugt und verwaltet werden. (z.B. Yubikey FIPS Authentisierungsgeräte). Die Erstellung des privaten Schlüssels geschieht vor Ort 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 AIS 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.

3.3 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 Unterschriftsregelungen 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.

3.4 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. Ein Revokationsantrag wird mittels der hinterlegten Mobilnummer und Freigabe überprüft. Weitere Verfahren zur Revokation sind gemäss Bestimmungen der CP/CPS möglich.

4 Leistungsdarstellung und Verantwortlichkeiten

Einmalige Leistungen

Tätigkeiten (S = Swisscom/T = Teilnehmer)		S	T
Bereitstellung des Service			
1.	Bereitstellung der AIS 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.	Zusenden der unterzeichneten Konfigurations- und Annahmeerklärung mit aktivierungsrelevanten Informationen und den geforderten Ansprechpartnern		✓
4.	Umsetzung der Auflagen der Konfigurations- und Annahmeerklärung		✓
5.	Bereitstellung eines vom Siegelersteller unterzeichneten Antrages zum Siegelzertifikat mit allen notwendigen Dokumenten zur Überprüfung des Siegelerstellers sowie der Zustimmung zu den Nutzungsbestimmungen des Service. Unterschrift im Antrag zum Siegelzertifikat durch einen für den Siegelersteller zeichnungsberechtigten Vertreter. Veranlassung der Identifikation durch persönliches Erscheinen eines Vertreters des Siegelerstellers oder durch qualifizierte elektronische Signatur.		✓
6.	Sicherstellung der Zusendung eines Zugangszertifikates an Swisscom durch den Siegelersteller oder dessen Bevollmächtigten mit Bestätigung der Vollmacht.		✓
7.	Erstellung und Verwaltung des privaten Schlüssels zum Zugangszertifikat in einem mit Swisscom oder seinem Partner abgesprochenen, kryptographischen Modul oder HSM mit Zertifizierung FIPS 140-2 durch den Siegelersteller, sofern qualifizierte elektronische Siegel erstellt werden. Die Erstellung des privaten Schlüssels auf dem HSM Device geschieht in Gegenwart eines autorisierten Vertreters von Swisscom und eines autorisierten Vertreters des Kunden. Die Erstellung und Übergabe des Zugangszertifikates wird im gemeinsam unterzeichneten Protokoll festgehalten. Der im Antrag benannte und befugte Vertreter oder die Vertreter müssen bei der gemeinsamen Erstellungszeremonie vertreten sein.	✓	✓
8.	Freischaltung der Kommunikation für das zugesendete Zugangszertifikat.	✓	
9.	Ggfs. Konfiguration der Firewall, serverseitig beim Teilnehmer.		✓
10.	Benennung eines Verantwortlichen inklusive laufender Stellvertretung für alle Fragen bezüglich der Technik und Sicherheit der Teilnehmerapplikation und Ansprechpartner für Auditfragen in der Konfigurations- und Annahmeerklärung.		✓

Tätigkeiten (S = Swisscom/T = Teilnehmer)	S	T
11. Prüfung der Antragsunterlagen.	✓	
12. Aufschalten des Teilnehmers und Zusenden der teilnehmerspezifischen Zugangsdaten.	✓	
13. Einbindung des AIS Services in die teilnehmerspezifische Anwendung(en) bzw. teilnehmerseitige Anbindung der Schnittstelle zum AIS, z.B. durch Einsatz einer Teilnehmerapplikation eines Partners.		✓
14. Prüfung des Zugriffs auf den AIS Service und der Angaben auf dem Siegelzertifikat. Umgehende Meldung allfälliger Fehler an Swisscom, bevor dieses für eine Siegelerstellung benutzt wird.		✓
15. Fehlerbehebung durch Update oder Neuinstallation.	✓	
16. Betrieb einer Revokationsstelle zur Ungültigkeitserklärung eines Siegelzertifikates bei Kompromittierung oder aus anderen Gründen	✓	
17. Revozieren und Ermöglichung von Revokationen durch den Siegelersteller bei Anzeichen einer Kompromittierung vom Siegel- oder Zugangszertifikat über ein von Swisscom publiziertes Revokationsverfahren.		✓
18. Meldung der Aufgabe der Geschäftstätigkeit sowie eine gegen den Teilnehmer gerichtete Konkursandrohung, die erfolgte Konkurseröffnung oder eine Nachlassstundung.		✓
Beendigung des Service oder Beendigung der Siegelerstellung für einen Siegelersteller		
1. Löschen der Siegel- und Zugangszertifikate in der AIS Infrastruktur.	✓	
2. Löschen der zugehörigen Schlüssel aus dem HSM.	✓	

Wiederkehrende Leistungen

Tätigkeiten (S = Swisscom/T = Teilnehmer)	S	T
Standardleistungen		
1. Betrieb der AIS Infrastruktur, Erneuerung des Siegelzertifikates rechtzeitig vor Ablauf der Gültigkeit.	✓	
2. LifeCycle Management der AIS 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. Auswahl eines kryptographischen Moduls oder HSMs im Falle eines geregelten Siegels, dass die Sperrung des Zugriffs auf die Teilnehmerapplikation spätestens nach 5 Fehlversuchen zur Authentisierung am Service ermöglicht. Es muss danach ein neues Zugangszertifikat in einer gemeinsamen Zeremonie mit Swisscom erstellt werden.		✓
9. Erstellung von Siegelzertifikaten	✓	
10. Festlegung der Siegelzertifikatsinhalte und Verfahren zur Siegelerstellung.	✓	

Tätigkeiten (S = Swisscom/T = Teilnehmer)	S	T
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 elektronischen Zeitstempel	✓	
14. Sicherstellen der Mitwirkungsleistungen und Auflagen durch den Sicherheitsverantwortlichen.		✓
15. Kundeninformation bei Störungen und Wartungen.	✓	
16. Bereitstellung der Supportdienstleistungen (Service Desk, Incident Management usw.)	✓	
17. Melden von Mutationen der teilnehmerspezifischen Informationen (Kontaktpersonen, Zugangszertifikat, Wegfall vom Siegelerstellern, 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 AIS Service betrifft		✓
21. Melden von Sicherheitsvorfällen auf dem System des Signaturservice, die Auswirkung auf den Teilnehmer oder Siegelersteller hat	✓	
22. Entscheid und Verantwortung für rechtliche Wirkungen der gewählten Siegelart (vgl. Kapitel 7.3).		✓
23. 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.	✓	
24. Anpassung der Schnittstelle an die neuen Vorgaben von Swisscom binnen von 3 Monaten.		✓

5 Service Level und -Reporting

5.1 Service Level

Die nachfolgenden Service Levels beziehen sich grundsätzlich auf die vereinbarte Support Time. Definitionen der Begriffe (Operation Time, Support Time, Availability, Security und Continuity) sowie die Beschreibung des Messverfahrens und des Reportings ergeben sich aus den übrigen Vertragsbestandteilen (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			
Operation Time	Mo-So 00:00-24:00		●
Provider Maintenance Window	PMW-DC	PMW Data Center Swisscom	●
	PMW-S: mit Vorankündigung für sicherheits- und systemkritische Updates	Täglich 19:00-07:00, nur für angekündigte Wartungen	●

Service Level & Zielwerte			Elektronische Siegel
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			
	Advanced (ITSLA)		●
	Customized (ITSLC)		○
Continuity			
ICT Service Continuity (ICTSC)[3]	RTO 120 h | RPO 24 h		●
	RTO 48 h | RPO 24 h		○
ICT Business Continuity (ICTBC)[4]			—

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

5.2 Service Level Reporting

Im Umfang des Service erhält der Teilnehmer den folgenden Standard Service Level Report. Weitere Reports können nach vorgängiger Machbarkeitsklärung der Kundenanforderungen kostenpflichtig mit dem Advanced Reporting angeboten werden.

Service Level Report		Elektronische Siegel	Berichts-Periode
Availability	Service Availability des Service ▪ Signaturservice	● (Auf Anfrage)	Monatlich
	▪ Verzeichnisdienste	● (Auf Anfrage)	Monatlich
Continuity	ICT Service Continuity RTO|RPO	● (Auf Anfrage)	Monatlich

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

6 Rechnungsstellung und Mengenreport

6.1 Rechnungsstellung

Die Rechnungsstellung erfolgt jeweils rückwirkend für den vergangenen Monat. Die Details zur Rechnungsstellung werden im Service Vertrag geregelt.

6.2 Mengenreport

Mengenreports werden im Service Vertrag geregelt.

[1] Wurde der AIS 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 SLA-Definitionen"
[3] RTO und RPO beziehen sich nur auf die Bereitstellung des AIS Service am SAIP. Mobilfunkdienste, die für die Identifikation, Authentifikation oder Willensbekundung genutzt werden sind hier nicht erfasst.
[4] Der AIS Service kann nicht mit dem Swisscom ICT Business Continuity Service für eine Business Continuity Lösung kombiniert werden.

7 Besondere Regelungen

7.1 Teilnehmerapplikation

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

7.2 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 Siegelerstellers oder durch die bisherige Vertreterin 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 Siegelerstellen berechtigt war oder irrtumsfrei erfolgt ist.

7.3 Einsatzmöglichkeiten des fortgeschrittenen oder qualifizierten Siegels

Die Verwendung des fortgeschrittenen oder qualifizierten 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 qualifizierten 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.

Qualifizierte elektronische Siegel (Zertifikat der Swisscom-Klasse Diamant): Das über den AIS erstellte qualifizierte elektronische Siegel erfüllt die in der CP/CPS definierten Eigenschaften und die Definition gemäss Art. 3 Ziff. 27 eIDAS-VO mit den Rechtswirkungen gemäss Art. 35 eIDAS-VO.

Fortgeschrittenes elektronisches Siegel (Zertifikat der Swisscom-Klasse Saphir): Das über den AIS erstellte fortgeschrittene elektronische Siegel erfüllt die in der CP/CPS definierten Eigenschaften und die Definition gemäss Art. 3 Ziff. 26 eIDAS-VO mit der Rechtswirkung gemäss Art. 35 eIDAS-VO.

Einfacher elektronischer Zeitstempel: Der über den AIS erstellte einfache elektronische Zeitstempel erfüllt die in der CP/CPS definierten Eigenschaften und die Definition gemäss Art. 3 Ziff. 33 eIDAS-VO mit den Rechtswirkungen gemäss Art. 41 eIDAS-VO. Es handelt sich nicht um einen qualifizierten elektronischen Zeitstempel gemäss Art. 3 Ziff. 34 eIDAS-VO.

Weder das fortgeschrittene elektronische Siegel noch das qualifizierte 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 qualifiziertes elektronisches Siegel ggfs. mit einem elektronischen Zeitstempel, damit beabsichtigte Rechtswirkungen überhaupt eintreten können.

Über AIS gemäss den Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten ausgestellte elektronische Siegel von den Issuing CAs "Diamant“ (qualifiziert) und „Saphir“ (fortgeschritten) können bei Anwendbarkeit anderen Rechts als dem EU-Recht abweichende, allenfalls weitergehende oder weniger weitgehende Wirkungen entfalten als dies nach EU-Recht der Fall ist.

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

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

Swisscom ITSF zieht für die Erbringung der Vertrauensdienste Swisscom (Schweiz) AG mit Sitz in der Schweiz bei. Swisscom (Schweiz) AG betreibt die IT-Systeme zur Erbringung der Vertrauensdienste und diese Systeme stehen in der Schweiz. Die digitalen Zertifikate werden somit auf Servern in der Schweiz ausgestellt. Es handelt sich deshalb um Auftragsdatenbearbeitung in der Schweiz durch Swisscom (Schweiz) AG, die im Auftrag von Swisscom ITSF erfolgt. Swisscom ITSF hat die hierfür erforderlichen datenschutzrechtlichen Vereinbarungen mit Swisscom (Schweiz) AG abgeschlossen. Eine Datenbearbeitung durch von Swisscom beigezogene Dritte und/oder aus dem Ausland erfolgt ausschliesslich im Einklang mit den einschlägigen Vorschriften der EU Datenschutzgesetzgebung. Solche Bearbeitungen können insbesondere durch Mitarbeitende mit Wohnsitz im Ausland (Grenzgänger) oder auf Reisen sowie durch Wartungsabteilungen ausländischer Herstellerfirmen stattfinden. Im Rahmen des vorliegenden Service sind namentlich folgende Konstellationen von einer solchen Bearbeitung betroffen:

- Der 3rd Level Support des Applikationsherstellers hat in Supportfällen aus der EU VPN-Zugriff auf Applikationsdaten bei Swisscom, die keine ausser den vom Siegelersteller im Zertifikat veröffentlichten Daten keine Personendaten beinhalten. Der Zugriff wird von Swisscom überwacht. Identifikationsdaten können vom Applikationshersteller nicht eingesehen werden.
- 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 in der Schweiz statt.
- RA-Agenten, die im Auftrag der Swisscom mit der RA-App Identifikationen durchführen, werden vom Kunden der Swisscom vorgeschlagen. Sie werden der Datenschutzverpflichtung unterworfen. Auch hier kann die Identifikation durch Ausländer, im Ausland oder durch im Ausland wohnende Grenzgänger erfolgen.
- Daten aus dem Identifikationsprozess, die mit der RA-App bearbeitet werden, können je nach Situation vom RA-Agenten auch im Ausland erhoben werden.

Im Rahmen des vorliegenden Service kann Swisscom im Falle von Störungen, welche Swisscom nicht selbst lösen kann, Hersteller/Wartungspartner aus der EU temporär und kontrolliert VPN-Zugriff auf die Systeme von Swisscom zum Zwecke der Störungsanalyse/-behebung gewähren. Dabei können in Einzelfällen auch die vom Siegelersteller im Zertifikat veröffentlichten Siegelerstellungsdaten und Stammdaten des Siegelerstellers (z.B. Organisationsname, Bezeichnung des vom Kunden 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.