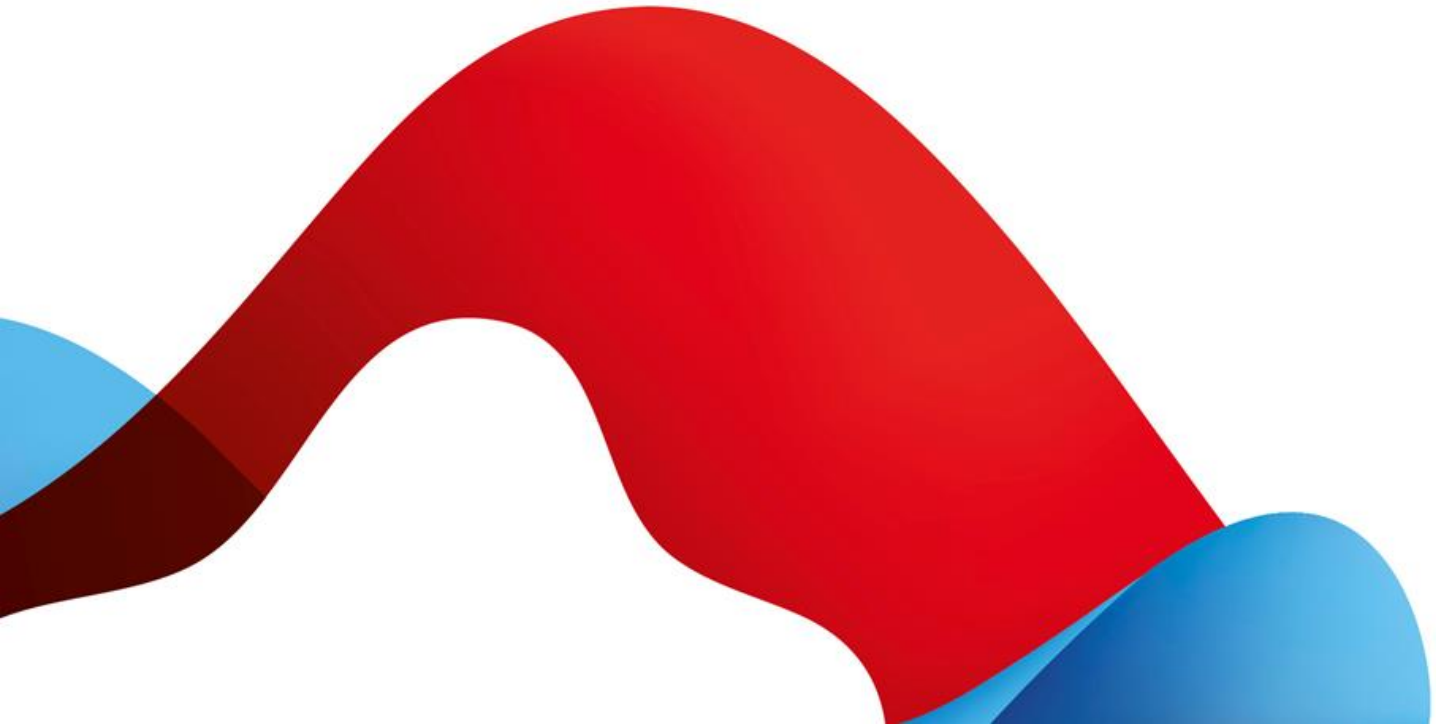
Leistungsbeschreibung

All-in Signing Service für Schweizer Personensignaturen (On-demand Signaturen)

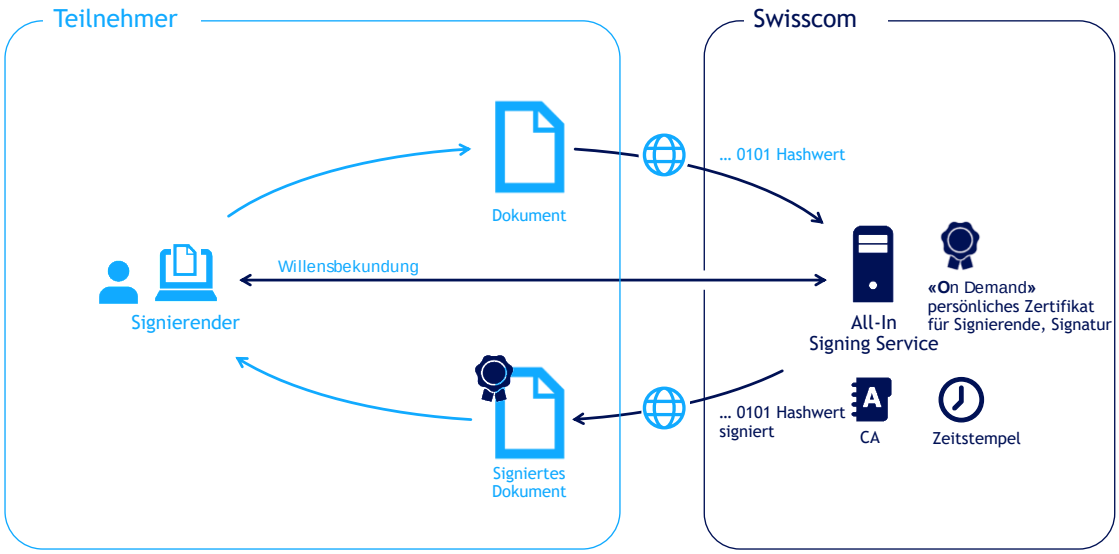


Inhaltsverzeichnis

1 Übersicht zum Service

Der All-in Signing Service (AIS) gemäss dieser Leistungsbeschreibung ist eine serverbasierte Fernsignaturdienstleistung, die in den Rechenzentren von Swisscom (Schweiz) AG in der Schweiz bereitgestellt wird. 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 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 AIS 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 All-In Signing Service nutzt hier eine Anfrage an das Mobiltelefon, z.B. mit Mobile ID in der Schweiz oder international per SMS mit Einmalpasswort.



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 7.1).

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.

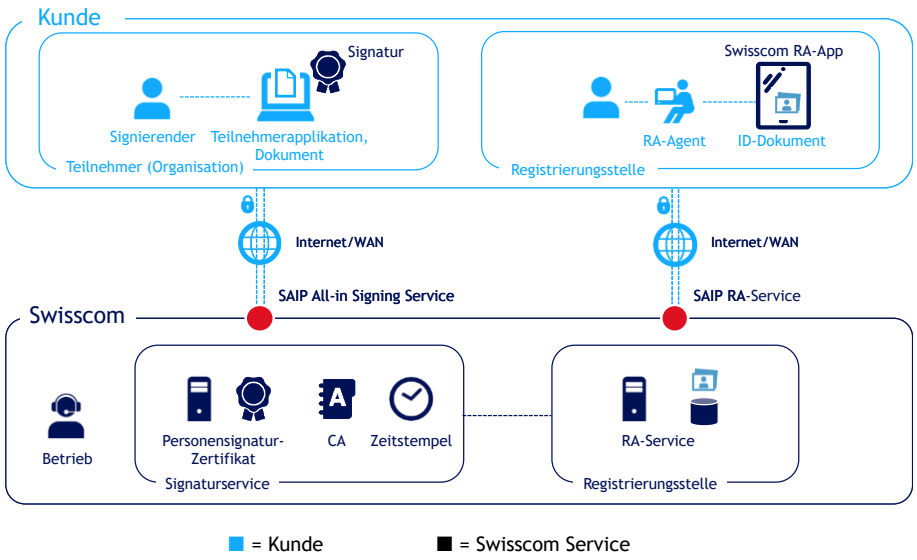
Allgemein bietet AIS je nach Vertragsgestaltung und nach Wahl des Teilnehmers fortgeschrittene elektronische Signaturen für natürliche oder juristische Personen sowie qualifizierte elektronische Signaturen für natürliche Personen an. Diese Leistungsbeschreibung beschreibt den Service für elektronische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

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:



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

2.2 Servicespezifische Definitionen

Begriff	Beschreibung
AIS Service	All-In Signing Service
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.
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 Dokumenteninhalt gezogen werden.

Begriff	Beschreibung
Mobile ID	Managed Service für die sichere Benutzer-Authentisierung. Mobile ID kann von verschiedenen Providern, unter anderem Swisscom, bezogen werden.
Nutzungsbestimmungen	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://www.swissdigicert.ch 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 (**R**egistration **A**uthority) Zuständige Stelle für die Identifikation der Signierenden. 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 Signaturerstellungs-Einheit (HSM)	Qualifizierte und zertifizierte Hardware zur Erstellung von Signaturschlüsseln und Signaturzertifikaten.
Signierender	Natürliche Person, die bei vorgängiger Identifikation, Authentifikation und Willensbekundung ein Dokument elektronisch signiert.
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 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. Diese Annahme- und Konfigurationserklärung gilt als "Subscriber Agreement" gemäss den ETSI Normen EN 319 411 für Vertrauensdienstanbieter.

Begriff	Beschreibung
Teilnehmerapplikation	Der Teilnehmer gibt den Signierenden Zugang zu einer Applikation, mit der sie elektronische Signaturen gemäss den Nutzungsbestimmungen von Swisscom 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 All-In Signing Service z.B. durch Partner bereitgestellt.
ZertES	Schweizerisches Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate

3 Ausprägungen und Optionen

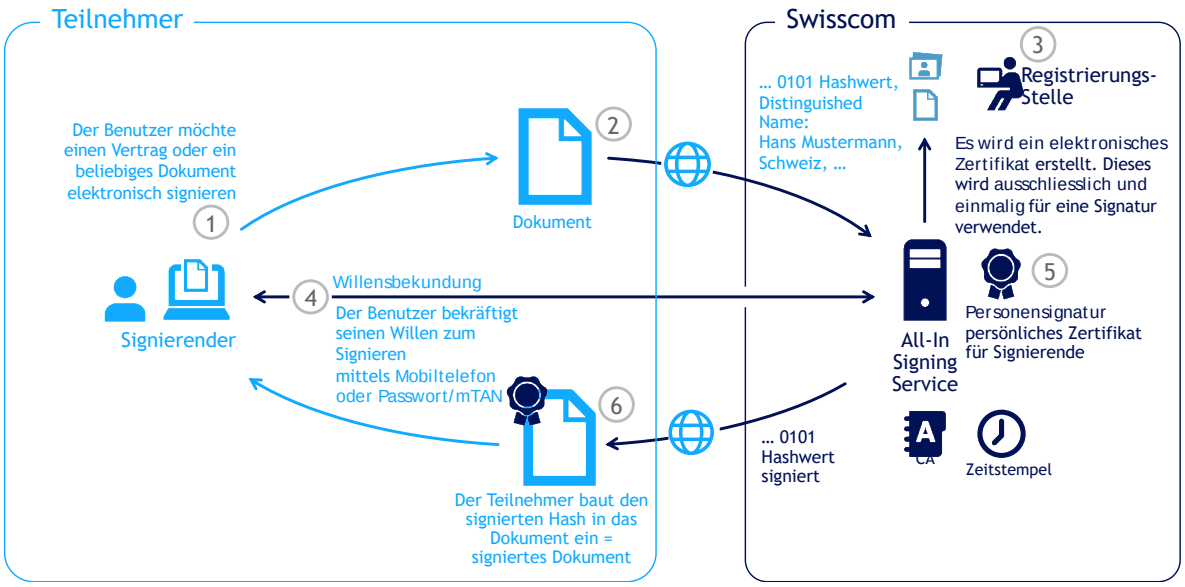
Standardausprägung	Elektronische Personensignaturen
Qualifizierte elektronische Signatur	●
Fortgeschrittene elektronische Signatur	●
Qualifizierter elektronischer Zeitstempel	●
Identifikation mit RA-App	●
Identifikation mit Videoidentifikation	○
Weitere vom Standard abweichende Identifikationsverfahren	○
Weitere vom Standard (Mobile ID, PWD/OTP) abweichende Willensbekundungsverfahren	○
Datenaufbewahrung in der Schweiz	●
Betrieb gemäss Zertifikatsrichtlinien (CP/CPS)	●

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

3.1 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
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)	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 aktuellsten Fassung hier aufgerufen werden: http://www.swissdigicert.ch/download_docs (Spalte "Schweiz (CH)")

3.1.1 Ablauf der Signaturerstellung für alle Optionen



- Applikation des Teilnehmers ist unter Verwendung eines SSL/TLS Zugangszertifikat mit der Swisscom AIS Plattform verbunden.
- Der Signierende, der bereits für den Service direkt oder via 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 AIS Plattform. Weiterhin werden auch für das Signaturzertifikatsubject relevante Angaben (Distinguished Name) von der Teilnehmerapplikation übergeben.
- Sofern die Registrierungsstelle der Swisscom mit der RA-App genutzt wurde, erfolgt ein Abgleich der mit vom Teilnehmer übermittelten Signaturdaten mit den Identifikationsdaten der Swisscom Registrierungsstelle. (3)
- Sofern der Teilnehmer von der Registrierungsstelle erfasst und für die Signatur zugelassen ist, fordert der AIS die Willensbekundung des Signierenden an. (4)
- Die Willensbekundung des Signierenden mittels Mobiltelefon oder Passwort / One Time Passwort (nachfolgend "PWD/OTP") wird ausgelöst. Qualifizierte Zertifikate und Signaturen werden ausschliesslich auf Basis einer 2-Faktor Authentisierung erstellt, welche mit Mobile-ID oder PWD/OTP erfolgt.
- 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 AIS Plattform bei Swisscom erzeugt und verwendet. Zu diesem Schlüsselpaar wird ein entsprechendes fortgeschrittenes bzw. qualifiziertes Zertifikat gemäss den Zertifikatsrichtlinien der Swisscom und dem von der Teilnehmerapplikation übergebenen Subjekt des Zertifikates (Distinguished Name) ausgestellt. Das Zertifikat und das Schlüsselpaar werden für einen einzigen Signaturaufruf 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)

3.2 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 an einer sogenannten Registrierungsstelle erfolgen und Swisscom bietet hierfür mehrere Varianten an.

3.2.1 Übersicht

Identifizierungsverfahren	Geeignet für qualifizierte Signatur CH	Geeignet für fortgeschrittene Signatur CH	
Standardverfahren RA-App nach 3.2.2	✓	✓	
Standardverfahren Videoidentifizierung nach 3.2.3	(✓)	✓	In der Schweiz nur im Kontext von Art. 7 Abs. 1 und 2 VZertES.
Eigene Registrierungsstelle mit abweichenden Identifizierungsverfahren	(✓)	(✓)	Je nach gesonderter Vereinbarung im Umsetzungskonzept und im Vertrag zur Delegation der Personenidentifikation

3.2.2 Standardverfahren RA-App mit separatem Vertrag

Swisscom stellt für die Durchführung der Personenidentifikation der Signierenden eine RA-App zur Verfügung. Die Bedienung erfolgt durch RA-Agenten, die in der Regel der Organisation des Teilnehmers oder die einer vom Teilnehmer oder Swisscom vorgeschlagenen dritten Organisation angehören. Die Organisation, die die RA-Agenten stellt, wird "RA-Agentur" genannt und sie schliesst einen gesonderten RA-Agentur-Vertrag ab. Die RA-Agentur verpflichtet sich vertraglich Swisscom gegenüber, mit der Nutzung der zur Verfügung gestellten App die Personenidentifikation im Auftrag und Namen von Swisscom entsprechend der Prozessvorgaben von Swisscom durchzuführen und diese der Registrierungsstelle bei Swisscom zu übertragen. Jeder RA-Agent erhält hierzu nach erfolgreicher Schulung eine Auflistung seiner Vertraulichkeits- und Mitwirkungspflichten zugesendet. Mit der unter Android und iOS lauffähigen RA-App verbleibt damit die Registrierungsstelle bei Swisscom. Swisscom ist jederzeit und ohne Grundangabe berechtigt, einem RA-Agenten seinen Status als RA-Agent und damit die Berechtigung dieser Person, die RA-App zu bedienen, fristlos zu entziehen.

Die RA-App fordert den RA-Agenten auf, zunächst den ausstellenden Staat und die Art (ID, Pass) des Identifizierungsdokumentes zu wählen. Es werden dann auf einem Muster des gewählten Dokumentes die Zonen für die haptische und visuelle Prüfung angezeigt, mit denen die Echtheit des Dokumentes geprüft werden kann. Anschliessend ist die Vorder- und Rückseite des Dokumentes zu fotografieren. Eine OCR ermittelt automatisch aus der maschinenlesbaren Zone des Dokumentes die notwendigen Identifikationsdaten. Diese müssen auf Lesefehler geprüft und korrigiert werden. Ein Foto der zu identifizierenden Person mit Hintergrund der Umgebung in der geprüft wurde (z.B. Tisch, charakteristische Wandbilder) beweist die physische Präsenz während der Prüfung. Die identifizierte Person erhält abschliessend einen Anruf auf eine zuvor eingegebene Mobiltelefonnummer, um die Korrektheit und Besitz der Mobiltelefonnummer zu bestätigen. Nach Abschluss der Identifikation muss die identifizierte Person die Nutzungsbestimmungen des AIS Service bestätigen, in dem sie den Link in einer zugesandten SMS des AIS Service anklickt und die dort angezeigten Bestimmungen bestätigt.

Eine Person, die durch die RA-App identifiziert wurde, wird damit „Community Member“ der Swisscom Signierenden und kann für die Dauer der Gültigkeit der Identifikation bei allen AIS-Teilnehmern der Swisscom eine gültige persönliche Signatur erstellen lassen, ohne dass eine erneute Identifikation notwendig ist, solange dies von der jeweiligen Teilnehmerapplikation zugelassen wird.

Swisscom kann RA-Master Agenten ernennen, die selbstständig weitere RA-Agenten innerhalb der gleichen Organisation vorschlagen können, so dass z.B. innerhalb einer Organisation ein ganzes Netzwerk von RA-Agenten aufgebaut werden kann. Die RA-Master Agenten unterliegen gesonderten Bestimmungen von Swisscom.

3.2.3 Standardverfahren Videoidentifizierung

Als weitere Identifikationsmöglichkeit bietet Swisscom diesen Service auch in Verbindung mit einer Videoidentifizierung an. Hierbei wird im Rahmen einer videobasierten Identifikationsfeststellung das vorzulegende Identifikationsdokument (z.B. Reisepass oder Identitätskarte) verifiziert und mit der im Video-Chat befindlichen Person durch autorisiertes Fachpersonal verglichen und geprüft. Die Identifikationsdaten werden zusammen mit den Authentifizierungsdaten dem All-in Signing Service übertragen, so dass bereits identifizierte Personen die Möglichkeit haben nur auf Basis des Authentifizierungsmittels zu signieren.

Im Schweizer Recht sind für die qualifizierte Signatur hierbei die Einschränkungen von Art. 7 Abs. 1 und 2 VZertES zu beachten. Technisch wird auch sichergestellt, dass dann qualifiziert die Signatur nur in der Signaturumgebung stattfinden kann, in der die Person identifiziert wurde. Die von Swisscom angebotene Registrierungsstelle mit Videoidentifizierung unterliegt einem gesonderten zusätzlichen Vertrag zu diesem Service und ist nicht Bestandteil dieser Leistungsbeschreibung (siehe Leistungsbeschreibung Digital Identification & Signing Service).

3.2.4 Projektspezifische Registrierungsstelle

Möchte der Teilnehmer die vorgenannten Verfahren zur Identifikation der Signierenden nicht einsetzen und eine eigene Registrierungsstelle mit projektspezifischer Identifizierung aufbauen oder sonst von den oben erwähnten Standardprozessen abweichen, so ist diese vorgängig mit Swisscom 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 Registrierungsstellenprozesse zusätzlich von der Anerkennungsstelle oder Konformitätsbewertungsstelle für Zertifizierungsdienste freigegeben werden.

3.2.5 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 Annahme- und Konfigurationserklärung 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.

3.3 Datenablage und Verantwortlichkeiten

3.3.1 Standardverfahren nach 3.2

Mit der Nutzung der von Swisscom zur Verfügung gestellten RA-App 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.

3.3.2 Projektspezifische Verfahren nach 3.2.4

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

3.4 Willensbekundung

Jede persönliche Signatur bedingt die Abgabe einer Willensbekundung durch den Signierenden. Für die Willensbekundung wird das Mobiltelefon mit der Mobiltelefonnummer verwendet, die bei der Identifikation des Signierenden angegeben wurde.

Für die Abgabe der Willensbekundung selber stehen 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 PWD/OTP Verfahren zurückgegriffen.
- PWD/OTP: Hierbei authentifiziert sich der Signierende über eine Passworteingabeseite, die er per SMS erhält, beim AIS Service und löst bei dem Service die Generierung eines Einmalpasswortes aus, das über SMS an das Mobiltelefon des Signierendes übermittelt wird. Dieses gibt der Signierende in die Teilnehmerapplikation ein.
- OTP: Bei diesem Verfahren entfällt die Authentisierung des Signierendes beim AIS Service, sondern der Signierende sendet direkt an den AIS Service ein Einmalpasswort, 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.

4 Leistungsdarstellung und Verantwortlichkeiten

4.1 Signaturservice

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 Annahme- und Konfigurationserklärung mit aktivierungsrelevanten Informationen und den geforderten Rollenbesetzungen (Systemadministrator, Sicherheitsbeauftragter und Master RA-Agent).		✓
4.	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.		✓
5.	Option Organisationseintrag im Signaturzertifikat: Prüfung der Berechtigung zum Führen des Organisationsnamens im Zertifikat.	✓	
6.	Zusenden eines öffentlich vertrauenswürdigen oder selbst signierten SSL/TLS-Authentisierungszertifikat zur Authentisierung gegenüber dem AIS Server und zur verschlüsselten Kommunikation mit dem AIS Service. Spezifikation siehe Annahmeerklärung.		✓
7.	Freischaltung der Kommunikation für das zugesendete Authentisierungszertifikat.	✓	
8.	Ggfs. Konfiguration der Firewall, serverseitig beim Teilnehmer.		✓
9.	Benennung eines Verantwortlichen inklusive laufender Stellvertretung für alle Fragen bezüglich der Technik, Sicherheit und Durchführung der Registrierung von Signierenden und Ansprechpartner für Auditfragen.		✓
10.	Aufschalten des Teilnehmers und Zusenden der teilnehmerspezifischen Zugangsdaten.	✓	
11.	Einbindung des AIS Services in die teilnehmerspezifische Anwendung(en) bzw. teilnehmerseitige Anbindung der Schnittstelle zum AIS, z.B. durch Einsatz einer Partnerapplikation.		✓
12.	Prüfung des Zugriffs auf den AIS Server und der Ausstellung von Signaturen. Umgehende Meldung allfälliger Fehler, bevor die Signaturen benutzt werden.		✓
13.	Fehlerbehebung durch Update oder Neuinstallation.	✓	
14.	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 AIS Infrastruktur.	✓	
2.	Löschen der Schlüssel aus dem HSM.	✓	

Wiederkehrende Leistungen

Tätigkeiten (S = Swisscom/T = Teilnehmer)	S	T
Standardleistungen		
1. Betrieb der AIS Infrastruktur.	✓	
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 etc.). 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 seines SSL/TLS-Authentisierungszertifikates rechtzeitiger Austausch bei Ablauf der Gültigkeit durch den benannten Sicherheitsverantwortlichen durch E-Mail an servicedesk.ict@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, PWD/OTP).		✓
10. Übermittlung der Daten des Signierenden (Distinguished Name) gemäss den Vorgaben in der Annahme- und Konfigurationserklärung.		✓
11. Durchführen von Signaturen für die eine Willensbekundung des Signierenden vorliegt.	✓	
12. Signatur in Verbindung mit einem qualifizierten Zeitstempel nach ZertES wird angeboten.	✓	
13. Sicherstellen der Mitwirkungsleistungen und Auflagen durch den Sicherheitsverantwortlichen.		✓
14. Bereitstellung der Supportdienstleistungen (Service Desk, Incident Management usw.)	✓	
15. Melden von Mutationen der teilnehmerspezifischen Informationen (Kontaktpersonen, SSL/TLS Zertifikat usw.)		✓
16. Nachführen der teilnehmerspezifischen Informationen (Kontaktpersonen, SSL/TLS Zertifikat usw.)	✓	
17. Melden von Sicherheitsvorfällen auf dem System der Teilnehmerapplikation, die den AIS Service betrifft.		✓
18. Melden von Sicherheitsvorfällen auf dem System des Signaturservice, die Auswirkung auf den Teilnehmer hat.	✓	
19. Entscheid und Verantwortung für rechtliche Wirkungen der gewählten Signaturart (vgl. Kapitel 7.1)		✓
20. Hinweis an die Signierenden über die verwendete Signaturart in der Benutzeroberfläche der Teilnehmeranwendung oder in der Frage der zur Willensbekundung		✓
21. Anpassung der Schnittstelle an die neuen Vorgaben von Swisscom binnen von 3 Monaten.		✓

4.2 RA-App zur Personenidentifikation

Tätigkeiten (S = Swisscom/T = Teilnehmer)	S	T
Leistungen bei optionaler Nutzung der RA-App		
1. Abschluss eines RA-Agentur-Vertrags mit der RA-Agentur Zwecks Ermöglichung der Vornahme der Personenidentifikation durch RA-Agenten unter Einsatz der Swisscom RA-App wie in Ziffer 3.2.2 dieser Leistungsbeschreibung beschrieben	✓	
2. Rücksprache mit der vom Teilnehmer vorgeschlagenen RA-Agentur zur Sicherstellung, dass eine allfällige Kündigung des RA-Agentur-Vertrags durch die RA-Agentur mit den Anforderungen des Teilnehmers übereinstimmt.		✓
3. Zusammenarbeit zur Erarbeitung und Integration eines neuen Identifikationsprozesses gemäss Möglichkeiten dieser Leistungsbeschreibung (vgl. Ziffer 3.2.1) bei Kündigung des RA-Agentur-Vertrags.	✓	✓

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 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			
Operation Time	Mo-So 00:00-24:00		●
Provider Maintenance Window	PMW-DC	PMW Data Center Swisscom	●
	PMW-S: mit Vorankündigung für sicherheits- und system-kritische Updates	Täglich 19:00-07:00, nur für angekündigte Wartungen	●
Support Time			
Support Time	Mo-So 00:00-24:00		●
Störungsannahme	Mo-So 00:00-24:00		●
Availability			
Service Availability			
Signaturservice	99.8%		●
Verzeichnisdienste nach CP/CPS Ziffer 3.1	99.9%		●
Security			
	Advanced (ITSLA)		●
	Customized (ITSLC)		○

Service Level & Zielwerte		Elektronische Personensignaturen
Continuity		
ICT Service Continuity (ICTSC) [1]	RTO 120 h | RPO 24 h	●
	RTO 48 h | RPO 24 h	○
ICT Business Continuity (ICTBC) [2]		—

● = Standard (im Preis inbegriffen) ○ = gegen Aufpreis — = nicht erhältlich

5.2 Service Level Reporting

Im Umfang des Service erhält der Kunde 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 Personensignaturen	Berichts-Periode
Availability	Service Availability des Service		
	▪ Signaturservice	● (Auf Anfrage)	Monat
	▪ Verzeichnisdienste	● (Auf Anfrage)	Monat
Continuity	ICT Service Continuity RTO|RPO	● (Auf Anfrage)	Monat

● = Standard (im Preis inbegriffen)

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 Servicevertrag geregelt.

7 Besondere Regelungen

7.1 Teilnehmerapplikation

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

7.2 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-Klasse Diamant): Die über den AIS 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 AIS erstellte qualifizierte elektronische Zeitstempel erfüllt die in der CP / CPS definierten Eigenschaften und die Definition gemäss Art. 2 Bst. j ZertES.

[1] 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.
[2] Der AIS Service kann nicht mit dem Swisscom ICT Business Continuity Service für eine Business Continuity Lösung kombiniert werden.

Fortgeschrittene elektronische Signatur (FES, Zertifikat der Swisscom-Klasse Saphir): Die über den AIS 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 AIS 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.

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

Die im Rahmen der Leistungserbringung vom Kunden an Swisscom übermittelten Daten (Kundendaten) 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:

- Der 3rd Level Support des Applikationsherstellers hat in Supportfällen aus der EU VPN-Zugriff auf Applikationsdaten bei Swisscom, die keine ausser den vom Signierenden 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 ausschliesslich 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 Signierenden im Zertifikat veröffentlichten Signaturdaten und Stammdaten der Kundenorganisation (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.

7.4 Support und Operation

Während der Supportzeit stellt Swisscom den Betrieb des AIS Service gemäss SLA Ziffer **Fehler! V erweisquelle konnte nicht gefunden werden.** bis zum SAIP sicher. Störungen können in dieser Zeit gemeldet und angenommen werden (1st Level Support). 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. Kundenspezifische Probleme, Serviceaufschaltungen und werden durch den 2nd Level Support Mo-Fr. während der Bürozeiten von 8h00 – 17h00 bearbeitet. Hierbei ist die Feiertagsregelung des Basisdokumentes "SLA-Definitionen" zu beachten.