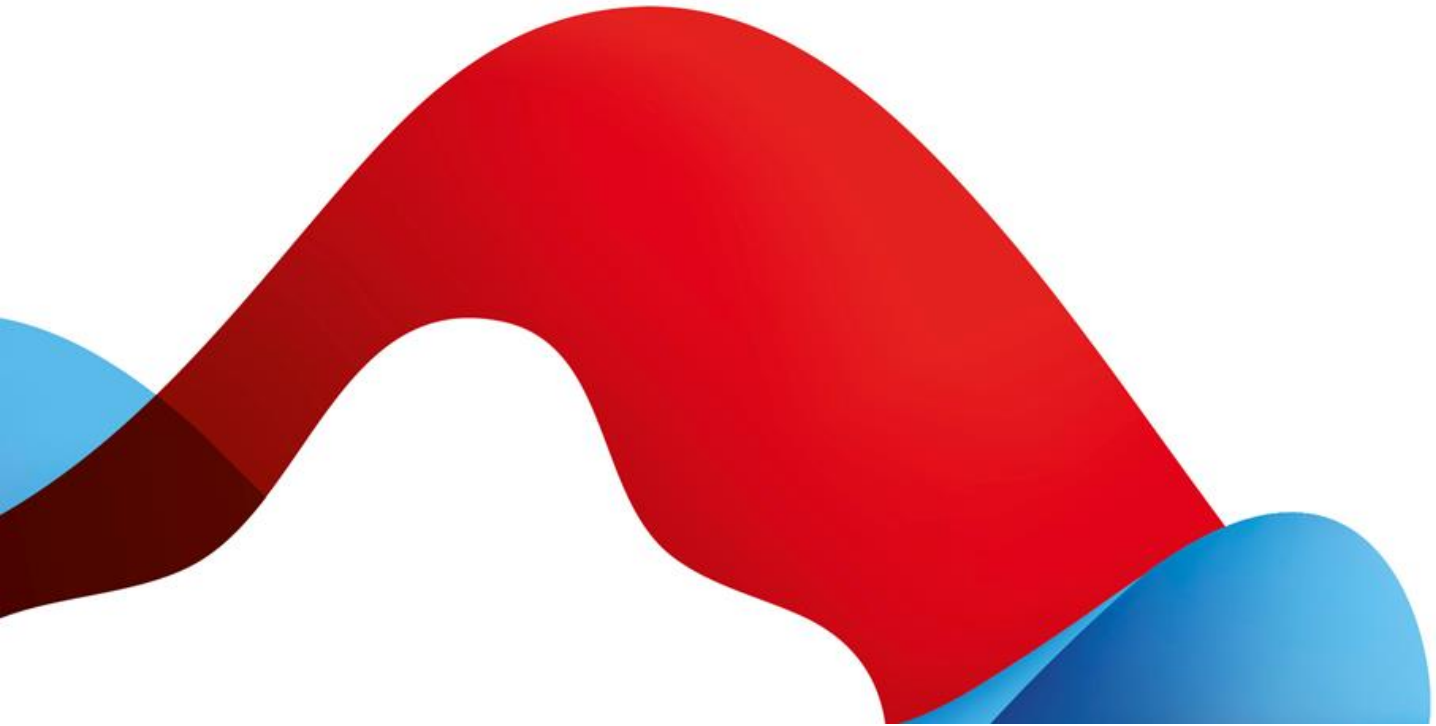
Leistungsbeschreibung

All-in Signing Service für EU Personensignaturen

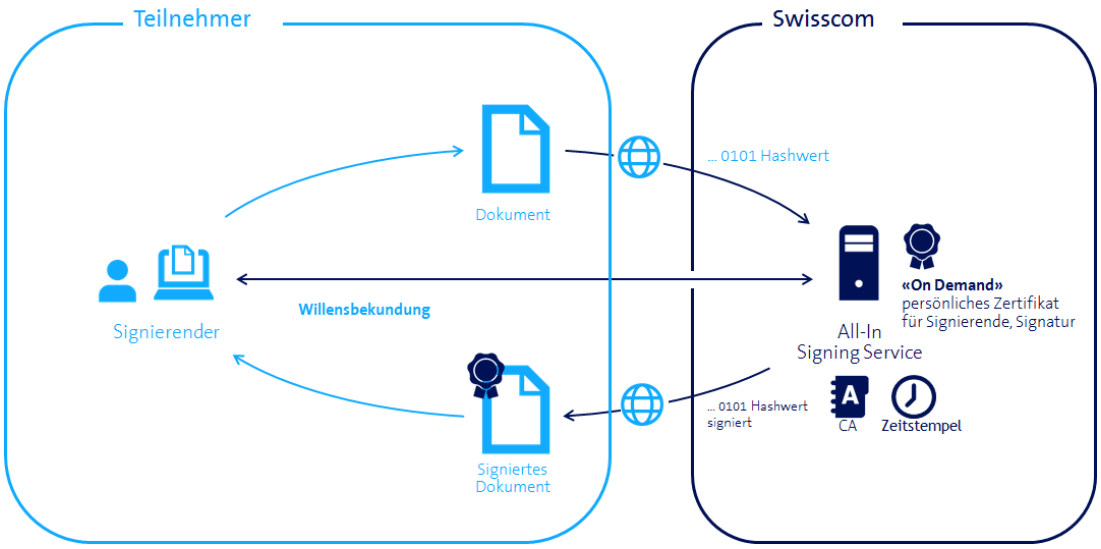


Inhaltsverzeichnis

1 Übersicht zum Service

Der All-in Signing Service (AIS) gemäss dieser Leistungsbeschreibung ist eine serverbasierte Fernsignaturdienstleistung der Swisscom IT Services Finance S.E., Wien (AT), nachfolgend "Swisscom ITSF" genannt. Der AIS wird in den Rechenzentren von Swisscom (Schweiz) AG in der Schweiz bereitgestellt wird und Swisscom (Schweiz) AG vertreibt den AIS in eigenem Namen oder räumt Dritten wiederum das Recht ein, den AIS in eigenem Namen zu vertreiben. Signierende können damit digitale Dateien elektronisch signieren und sichern damit die Integrität und die Authentizität einer Datei. Der qualifizierte Vertrauensdienst von Swisscom ITSF erzeugt und verwaltet unter Beizug von Swisscom (Schweiz) AG 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 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 für Swisscom nicht ersichtlich. Der signierte Hash wird von der Teilnehmerapplikation wieder in das Dokument eingebaut und erzeugt damit ein signiertes Dokument. Vor der Auslösung der Signatur muss der Teilnehmer sich an der Teilnehmerapplikation authentifizieren und den Willen zur Signatur bekunden. Der All-In Signing Service nutzt hier verschiedene mögliche Authentifizierungsverfahren.



Die Signierenden können sich vorgängig durch ein nach eIDAS zugelassenes Verfahren identifizieren (z.B. "RA-App", eigene Registrierungsstelle) und anschliessend bei jeder Signatur eine damit verbundene Authentifizierung nutzen.

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 7.2).

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

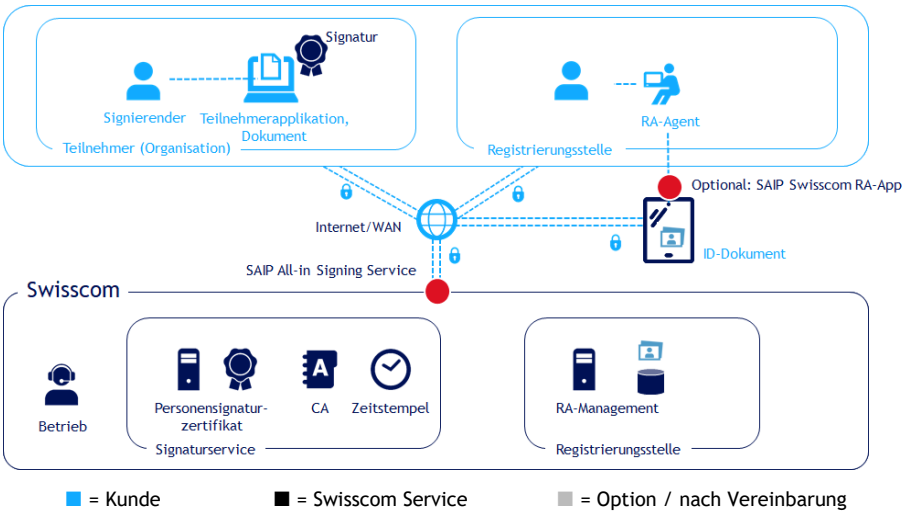
Allgemein bietet der AIS Service von Swisscom ITSF je nach Vertragsgestaltung und nach Wahl des Teilnehmers fortgeschrittene elektronische Signaturen sowie qualifizierte elektronische Signaturen für natürliche Personen und fortgeschrittene elektronische Siegel für juristische Personen an. Diese Leistungsbeschreibung beschreibt den Service für elektronische Signaturen für natürliche Personen in der EU und EWR Staaten, die die eIDAS Verordnung umgesetzt haben.

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.

Begriff	Beschreibung
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 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.
Mobile ID	Managed Service für die sichere Benutzer-Authentisierung. Mobile ID kann in der Schweiz von verschiedenen Providern, unter anderem Swisscom (Schweiz) AG, bezogen werden.
Nutzungsbestimmungen	Die Nutzungsbestimmungen regeln im Verhältnis zwischen Swisscom IT Services Finance S.E. 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	Registrierungsstelle (**R**egistration **A**uthority)
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)	Zuständige Stelle für die Identifikation der Signierenden. Kann vom Teilnehmer, Swisscom ITSF 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 eine elektronische Signatur beantragt und bei erfolgter Identifikation, Authentifikation und Willensbekundung auch signiert.
SOAP	Simple Object Access Protocol – Alternatives Schnittstellen Programmierparadigma zu REST für Webservices.

Begriff	Beschreibung
SSL/TLS	Secure Socket Layer, Transport Layer Security, Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet basierend auf SSL (Zugangs-) Zertifikaten.
Teilnehmer	Swisscom ITSF erbringt die Leistungen gemäss vorliegender Leistungsbeschreibung zu Gunsten des Teilnehmers. Der Teilnehmer ist entweder direkt Kunde von Swisscom (Schweiz) AG mit einem All-in Signing Service Vertrag (inklusive Konfigurations- und Annahmeerklärung gegenüber Swisscom ITSF) oder er hat einen kommerziellen Vertrag mit einem Partner von Swisscom (Schweiz) AG mit einer Konfigurations- und Annahmeerklärung gegenüber Swisscom ITSF. Diese Annahme- und Konfigurationserklärung gilt als "Subscriber Agreement" gemäss den ETSI Normen EN 319 411 für Vertrauensdienstanbieter.
Teilnehmerapplikation	Der Teilnehmer gibt den Signierenden Zugang zu einer Applikation, mit der sie elektronische Signaturen gemäss den Nutzungsbestimmungen von Swisscom ITSF erstellen können und der Teilnehmer stellt dabei neben der Authentisierung die Übertragung der Signaturdaten zum Fernsignaturservice von Swisscom ITSF 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.

3 Ausprägungen und Optionen

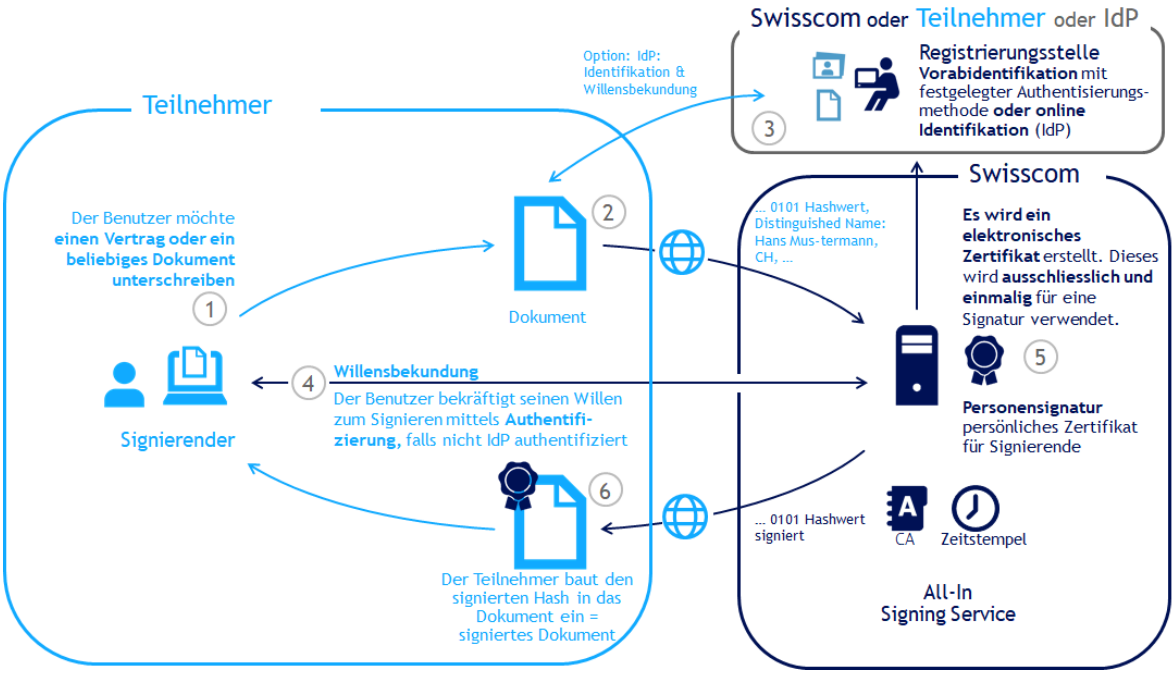
Standardausprägung	Elektronische Personensignaturen
Qualifizierte elektronische Signatur	●
Fortgeschrittene elektronische Signatur	●
Elektronischer Zeitstempel (nicht qualifiziert)	●
Identifikation mit RA-App	●
Weitere Identifikationsverfahren	○
Betrieb gemäss Zertifikatsrichtlinien (CP/CPS)	●

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

3.1 Definition der Leistungen

Leistung	Definition
Qualifizierte elektronische Signatur	Qualifizierte elektronische Signatur gemäss Art. 3 Ziff. 12 eIDAS-VO.
Fortgeschrittene elektronische Signatur	Fortgeschrittene elektronische Signatur gemäss Art. 3 Ziff. 11 eIDAS-VO.
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.
Betrieb gem. Zertifikatsrichtlinien (CP/CPS)	Der Betrieb eines Zertifizierungsdiensteanbieter richtet sich nach den EU-Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten der Klasse "Diamant“ (qualifiziert) und „Saphir“ (fortgeschritten). Diese können in der aktuellsten Fassung hier aufgerufen werden: https://www.swissdigicert.ch/download_docs (Spalte Europa "EU")

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 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 den AIS Service. Weiterhin werden auch für das Signaturzertifikatsubject relevante Angaben von der Teilnehmerapplikation übergeben.
- Sofern die Registrierungsstelle der Swisscom mit der RA-App genutzt wurde, muss der Signierende vor Nutzung der ersten Signatur erstmalig identifiziert werden und mit einer Willensbekundungsmethode (Authentifizierung) in Verbindung gebracht werden. Es erfolgt bei der Signatur 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)
- Qualifizierte Zertifikate und Signaturen werden ausschliesslich auf Basis einer 2-Faktor Authentisierung erstellt, z.B. basierend auf Mobile-ID, PWD/OTP oder einer anderen zertifizieren Authentisierungsmethode.
- Das Schlüsselmaterial (private und öffentliche Schlüssel) sowie Signaturzertifikate, welche für die fortgeschrittene bzw. qualifizierte elektronische Signatur (inkl. Zeitstempel) notwendig sind, werden erstellt. (5) Das Schlüsselmaterial wird – unter der Verantwortung von Swisscom ITSF auf dem AIS Service bei Swisscom (Schweiz) AG erzeugt und verwendet. Zu diesem Schlüsselpaar wird ein entsprechendes fortgeschrittenes bzw. qualifiziertes Signaturzertifikat gemäss den Zertifikatsrichtlinien der Swisscom ITSF und dem von der Teilnehmerapplikation übergebenen Subjekt des Signaturzertifikates (Distinguished Name) ausgestellt. Das Signaturzertifikat und das Schlüsselpaar werden für einen einzigen Signaturaufruf des Teilnehmers verwendet und das Schlüsselpaar nach dessen Verwendung gelöscht. Persönliche Signaturzertifikate 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 Signaturzertifikat (z.B. Zertifikatskette zum vertrauenswürdigen Root-Zertifikat sowie Zeitstempel). Die Teilnehmerapplikation stellt die Signatur des Dokumentes aufgrund des signierten Hashs sicher. (6)

3.2 Prozesse und Tools zur Personenidentifikation (Registrierungsstelle)

Bevor eine Willensbekundung 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 eIDAS	Geeignet für fortgeschrittene Signatur eIDAS	
Standardverfahren RA-App nach 3.2.2	✓	✓	
Standardverfahren Videoidentifizierung nach 0	(✓)	✓	Mit eIDAS notifiziertem Videoidentifikationsdienst optional möglich
Eigene Registrierungsstelle mit abweichenden Identifizierungsverfahren nach 3.2.4	(✓)	(✓)	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 jedes beliebigen Signierenden eine RA-App von Swisscom (Schweiz) AG zur Verfügung. Swisscom (Schweiz) AG ist von Swisscom ITSF als Registrierungsstelle benannt. 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 des zu identifizierenden potentiell Signierenden mit Hintergrund der Umgebung in der geprüft wurde (z.B. Tisch, charakteristische Wandbilder), beweist die physische Präsenz während der Prüfung. Der potentiell Signierende erhält abschliessend einen Anruf auf eine zuvor eingegebene Mobiltelefonnummer, um die Korrektheit und Besitz der Mobiltelefonnummer zu bestätigen. Nach Abschluss der Identifikation muss der Signierende die Nutzungsbestimmungen des AIS von Swisscom ITSF und wahlweise auch Swisscom(Schweiz) AG bestätigen, in dem sie die Links in einer per SMS zugesandten Webseite des AIS Service anklickt und die dort angezeigten Bestimmungen bestätigt und signiert.

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

Swisscom kann auf Vorschlag der RA-Agentur 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.

3.2.3 Standardverfahren Videoidentifizierung

Als weitere Identifikationsmöglichkeit kann der Service auch in Verbindung mit einer Videoidentifizierung durchgeführt werden. 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 Videoidentifizierung unterliegt einem gesonderten zusätzlichen Vertrag zu diesem Service und ist nicht Bestandteil dieser Leistungsbeschreibung. Sie kann von Swisscom mit Videoidentifizierer angeboten werden, wenn Swisscom ITSF damit die Voraussetzungen der eIDAS-VO erfüllt und die Aufsichtsbehörde dies bestätigt.

3.2.4 Projektspezifische Registrierungsstelle

Möchte der Teilnehmer das Verfahren zur Identifikation der Signierenden über die RA-App 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 einen Delegationsvertrag zur Identifikation für Personensignaturen (Vertrag RA-Delegation) mit Swisscom (Schweiz) AG abschliessen und bis zur Inkraftsetzung des Vertrages ein Umsetzungskonzept vorlegen, welches durch Swisscom geprüft und bewertet wird. In der Regel müssen eigene projektspezifische Registrierungsstellenprozesse für die Ausstellung von qualifizierten Signaturzertifikaten zusätzlich von der Konformitätsbewertungsstelle und der Aufsichtsstelle freigegeben werden.

3.2.5 Prozess zur Organisationsprüfung

Sofern bei dem vorgenannten Verfahren zur Personenidentifikation auch die mit dem potentiell Signierenden verbundene Organisation festgehalten wird, wird eine Organisationsprüfung gemäss Bestimmung der CP/CPS (siehe Ziffer 3.1) vor Aufnahme des Service von Swisscom ITSF durchgeführt. Hierzu muss die Organisation 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 Ziffer 3.2

Mit der Nutzung der RA-App werden die Daten zur identifizierten Person sowie die Identifikationsunterlagen und der Nachweis der Annahme der Nutzungsbestimmungen auf Servern der Registrierungsstelle, Swisscom (Schweiz) AG, in der Schweiz gespeichert und entsprechend den in der CP/CPS oder Gesetz genannten Fristen aufbewahrt.

3.3.2 Projektspezifische Verfahren nach Ziffer 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 die Authentisierungsmethode verwendet, die bei der Identifikation des Signierenden angegeben wurde, oder es wurde im Rahmen der Identifizierung bereits eine Willensbekundung geleistet.

Für die Abgabe der Willensbekundung selber stehen verschiedene Verfahren zur Verfügung:

- PWD/OTP: Hierbei authentifiziert sich der Signierende über eine Passwortseite, die er per SMS erhält, beim AIS Service und löst bei dem Service eine 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 Signierenden 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.
- Mobile ID: Derzeit nur einsetzbar mit MobileID-fähigen SIM Karten von Schweizer Mobilfunkanbietern. 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. Diese Variante ist auf einfachen Mobilgeräten durchführbar (d.h. kein Smartphone notwendig).

- 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. Alternativ Schnittstelle über OAuth2.0 nach Standard ETSI TS 119 432. 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).		✓
4.	Option Organisationseintrag im Signaturzertifikat: Bereitstellung auf Anforderung von Swisscom ITSF 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 Signaturzertifikat für die Signierenden einverstanden ist.		✓
5.	Option Organisationseintrag im Signaturzertifikat: Prüfung der Berechtigung zum Führen des Organisationsnamens im Signaturzertifikat.	✓	
6.	Zur Verfügungstellung eines öffentlich vertrauenswürdigen oder selbst signierten Zugangszertifikates zur Authentisierung gegenüber dem AIS Server und zur verschlüsselten Kommunikation mit dem AIS Service. Spezifikation siehe Annahmeerklärung.		✓
7.	Freischaltung der Kommunikation für den Teilnehmer auf Basis des zugesendeten Zugangszertifikates.	✓	
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/oder 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 ITSF/T = Teilnehmer)		S	T
Standardleistungen			
1.	Betrieb der AIS Infrastruktur.	✓	
2.	LifeCycle Management der AIS Service Infrastruktur.	✓	
3.	LifeCycle Management der Infrastruktur der mit dem All-in Signing Service verbundenen Systeme: Anpassung an den aktuellen Stand der Technik und Sicherheit (Security Patches, Updates, usw.).		✓
4.	Angemessene technische und organisatorische Massnahmen zum Schutz der übermittelten Daten (z.B. auch durch Abschaltung nicht benötigter Zugänge, Zugangsregelungen etc.). Offenlegung des Sicherheitsdispositivs der der Kommunikation, sofern von Swisscom ITSF oder dessen Konformitätsbewertungsstelle oder Aufsichtsstelle verlangt.	✓	✓
5.	Anpassung der Definition der Sicherheitsanforderungen.	✓	
6.	Lifecycle-Management seines Zugangszertifikates 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. Schweizer 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 Zeitstempel.	✓	
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, Zugangszertifikat usw.)	✓	
17.	Melden von Sicherheitsvorfällen auf dem System der Teilnehmerapplikation oder des IdP, 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 7.2)		✓
20.	Anzeige an den Signierenden, ob es sich um eine fortgeschrittene oder qualifizierte Signatur handelt		✓
21.	Anpassung der Schnittstelle an die neuen Vorgaben von Swisscom ITSF binnen von 3 Monaten aufgrund regulatorischer oder sicherheitstechnischen Notwendigkeiten		✓

4.2 RA-App zur Personenidentifikation

Einmalige Leistungen

Tätigkeiten (S = Swisscom/T = Teilnehmer)	S	T
Standardleistungen		
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.	✓	✓

Wiederkehrende Leistungen

Tätigkeiten (S = Swisscom/T = Teilnehmer)	S	T
Standardleistungen		
1. Identifikation der Signierenden, Aufschaltung weiterer RA-Agenten gemäss RA-Agentur Vertrag		✓
2. Freischaltung der Signierenden für die Signatur, Betrieb eines Portals zur Verwaltung und Registrierung aller RA-Agenten, weiterer Master-RA-Agenten und signierten Personen	✓	

4.3 Eigene Registrierungsstelle, IdP, Videoidentifikation

Einmalige Leistungen

Tätigkeiten (S = Swisscom/T=Teilnehmer)	S	T
Standardleistungen		
1. Abschluss eines Vertrages zur Delegation der Personenidentifikation ("RA-Delegationsvertrag") zwecks Ermöglichung der Vornahme der Personenidentifikation durch eine eigene Registrierungsstelle gemäss eine, Umsetzungskonzept und/oder Zertifizierungen	✓	
2. Erstellung eines Umsetzungskonzeptes zum Betrieb der Registrierungsstelle mit relevanten Angaben (Registrierungsprozess, Zustimmung zur Nutzungserklärung, Archivierung der Registrierungsdaten, Datenübergabe nach Aufgabe der Geschäftstätigkeit, Registrierungsverantwortliche und -Organisation, System- und Netzwerksicherheitskonzept, Datenschutz) und/oder einer entsprechenden Zertifizierung gemäss ETSI (fortgeschritten) oder eIDAS (qualifiziert)		✓
3. Zusammenarbeit zur Erarbeitung und Integration eines neuen Identifikationsprozesses gemäss Möglichkeiten dieser Leistungsbeschreibung (vgl. Ziffer 3.2.1) bei Kündigung des RA-Delegationsvertrags.	✓	✓

Wiederkehrende Leistungen

Tätigkeiten (S = Swisscom/T=Teilnehmer)	S	T
Standardleistungen		
1. Identifikation der Signierenden		✓
2. Ermöglichung der identifizierten Signierenden zur digitalen Signatur	✓	✓

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 systemkritische 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)		○
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 Teilnehmer den folgenden Standard Service Level Report. Weitere Reports können nach vorgängiger Machbarkeitsklärung der Teilnehmeranforderungen kostenpflichtig mit dem Advanced Reporting angeboten werden.

[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.

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 Service Vertrag 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 ITSF oder Swisscom (Schweiz) AG 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. 3 Ziff. 12 eIDAS-VO mit den Rechtswirkungen gemäss Art. 25 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.

Fortgeschrittene elektronische Signatur (FES, Zertifikat der Swisscom-Klasse Saphir): Die über den AIS erstellte FES erfüllt die in der CP / CPS definierten Eigenschaften und die Definition gemäss Art. 3 eIDAS-VO mit der Rechtwirkung gemäss Art. 25 Abs. 1 eIDAS-VO. Die FES hat nicht die gleichen Rechtswirkungen wie eine handschriftliche Unterschrift oder eine QES.

Je nach Situation benötigen gewisse Dokumente also die handschriftliche Unterschrift oder die QES ggfs. mit einem elektronischen Zeitstempel, damit beabsichtigte Rechtswirkungen überhaupt eintreten können.

Über AIS gemäss den Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten ausgestellte elektronische Signaturen 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 Signaturzertifikaten unterliegt zudem in/mit gewissen Staaten gesetzlichen Restriktionen.

7.3 Datenbearbeitung durch Dritte aus dem In- oder Ausland

Die im Rahmen der Leistungserbringung vom Teilnehmer an Swisscom übermittelten Daten werden grundsätzlich von Swisscom (Schweiz) AG in der Schweiz bearbeitet. Eine Datenbearbeitung durch von Swisscom (Schweiz) AG beigezogene Dritte und/oder von ausserhalb der Schweiz erfolgt ausschliesslich im Einklang mit den Vorschriften der einschlägigen Gesetzgebung. Solche Bearbeitungen können insbesondere durch Mitarbeitende mit Wohnsitz in der EU (Grenzgänger) oder auf Reisen sowie durch Wartungsabteil-

ungen von Herstellerfirmen aus der EU sowie auch durch Swisscom IT Services Finance S.E. aus Wien in ihrer Rolle als Vertrauensdiensteanbieterin stattfinden. Im Rahmen des vorliegenden Service sind namentlich folgende Konstellationen von einer solchen Bearbeitung betroffen:

- Swisscom IT Services Finance S.E. bearbeitet via Swisscom (Schweiz) AG diejenigen Daten, die erforderlich sind, um ihren Vertrauensdienst erbringen zu können, insbesondere für die Ausstellung der elektronischen Zertifikate.
- Der 3rd Level Support des Applikationsherstellers hat in Supportfällen aus der EU VPN-Zugriff auf Applikationsdaten bei Swisscom (Schweiz) AG, die keine ausser den vom Signierenden im Zertifikat veröffentlichten Daten Personendaten beinhalten. Der Zugriff wird von Swisscom (Schweiz) AG überwacht. Identifikationsdaten können vom Applikationshersteller nicht eingesehen werden.
- Aufsichtsbehörden und Konformitätsbewertungsstellen, welche die Konformität der Signaturanwendung für Swisscom IT Services Finance S.E. 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.
- 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 (Schweiz) AG im Falle von Störungen, welche sie nicht selbst lösen kann, Hersteller/Wartungspartner aus der EU temporär und kontrolliert VPN-Zugriff auf die Systeme 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 Zugangszertifikat) 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 in der Schweiz.

7.4 Support und Operation

Während der Supportzeit stellt Swisscom den Betrieb des AIS Service gemäss SLA Ziffer 5.1 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.