



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

Leistungsbeschreibung
RA Enterprise App Framework Service

Swisscom Trust Services

Swisscom Trust Services AG

Konradstrasse 12
8005 Zürich

Switzerland

<https://trustservices.swisscom.com>

E-Mail: sts.sale-support@swisscom.com



1	Inhalt	
1	Inhalt.....	2
2	Übersicht zum Service	3
3	Definitionen	4
3.1	Service Access Interface Point (SAIP).....	4
3.2	Servicespezifische Definitionen	4
4	Ausprägungen und Optionen.....	5
4.1	Definition der Leistungsausprägungen und Optionen.....	6
4.2	Ablauf der Identifizierung und Registration	6
4.2.1	Prozessbeschreibung Identifizierung und Registration	6
4.2.2	Webportal für RA-Master Agenten	8
4.2.3	Schnittstellen des Framework Service.....	8
4.2.4	Onboarding Prozess	9
4.2.5	Freigabeprozess	9
4.2.6	Wesentliche Punkte des Security Assessments.....	9
4.2.7	Release Management.....	9
4.3	Prozessbeschreibung RA Agenten Netzwerk und Schulungsprozess	10
4.4	Schulung und Sorgfalt bei der Identifizierung und Registration.....	10
5	Leistungsdarstellung und Verantwortlichkeiten	11
6	Service Level und -Reporting	12
6.1	Service Level	12
6.2	Service Level Reporting	13
7	Rechnungsstellung und Mengenreport	13
7.1	Rechnungsstellung.....	13
7.2	Mengenreport	13
8	Besondere Regelungen	14
8.1	Bereitstellung des Frameworks durch Swisscom	14
8.2	Anpassung Regulatorische Änderungen	14
8.3	Identifikation von Personen mit Wohnsitz ausserhalb EU/EWR/Schweiz.....	14



2 Übersicht zum Service

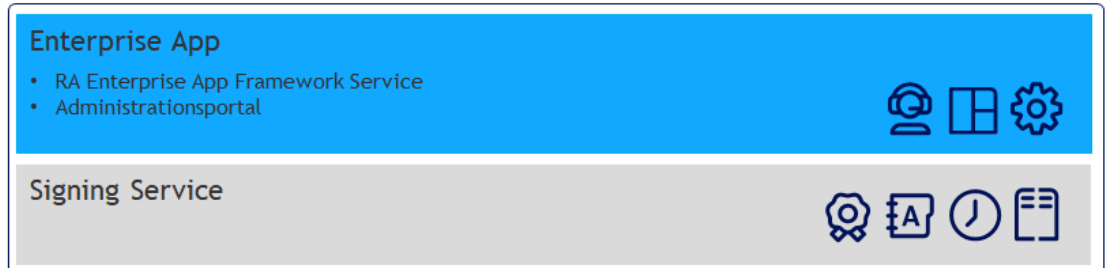
Der Signing Service gemäss dieser Leistungsbeschreibung ist eine serverbasierte Fernsignaturdienstleistung der Swisscom IT Services Finance S.E., Wien (AT), nachfolgend "Swisscom ITSF" genannt und der Swisscom (Schweiz) AG. Der Signing Service der Swisscom IT Services Finance S.E. wird in den Rechenzentren von Swisscom (Schweiz) AG in der Schweiz bereitgestellt und Swisscom Trust Services AG (nachfolgend „Swisscom“) vertreibt den Signing Service sowohl von Swisscom (Schweiz) AG für die Schweiz als auch von Swisscom IT Services Finance S.E. für die EU in eigenem Namen oder räumt Dritten wiederum das Recht ein, den Signing Service in eigenem Namen zu vertreiben.

Die Dienstleistung wird Teilnehmern zur Verfügung gestellt, die eine Teilnehmerapplikation, die RA Enterprise App, betreiben. Der Service zur Bereitstellung einer RA Enterprise App von Swisscom Frameworks (nachfolgend "**Framework Service**" genannt) ermöglicht für den Teilnehmer die Erstellung eigener Applikationen und Prozesse für die Registrierung von natürlichen Personen zur Signatur mit dem Signing Service. Der Framework Service wird durch Swisscom (Schweiz) AG bereitgestellt und ist Teil der Swisscom Vertrauensdienste. Registrierungen können sowohl für die fortgeschrittene und qualifizierte Signatur in der EU als auch in der Schweiz genutzt werden.

Konkret ermöglicht der Framework Service dem Teilnehmer, eine eigene Applikation für mobile Geräte (nachfolgend "**Enterprise App**" genannt) zu entwickeln, welche von ihm eingesetzt wird, um Geschäftsbeziehungen mit natürlichen Personen (nachfolgend «**zu identifizierende Person**» oder nach dem Identifikationsprozess «**identifizierte Person**» genannt) über einen direkten Präsenzkontakt aufzunehmen.

Die Enterprise App wird vom Teilnehmer oder einem vom Teilnehmer beauftragten Dritten selbst erstellt. Wichtige Funktionen zur Identifizierung werden dabei von Swisscom im Rahmen eines **Enterprise App Frameworks** (nachfolgend "**Framework**" genannt) zur Verfügung gestellt. Dabei sind die Anforderungen an die Registrierung aufgrund des Frameworks in der Enterprise App so abgebildet, dass die Registrierungsdaten – auf der Grundlage eines separaten **RA Delegationsvertrags für die RA Enterprise App** – vom Teilnehmer gleichzeitig auch als Registrierungsstelle für Swisscom als Zertifizierungsdienstanbieter erhoben und dem Zertifizierungsdienst und Trust Service von Swisscom zur Verfügung gestellt werden. Auf der Basis des Registrierungsprozesses und der Registrierungsdaten kann Swisscom ihren Dienst für elektronische Signaturen den registrierten Personen anbieten, ohne dass diese ein zweites Mal durch denselben Registrierungsprozess durchlaufen müssen.

Die Bereitstellung der Enterprise App erfolgt im Rahmen einer Dienstleistung, die die laufende Kontrolle der Funktionsfähigkeit und laufende Fehlerbehebung sowie Funktionsupdates sicherstellt. Für die Kontrolle der Daten im Rahmen der Signatur stehen dem Teilnehmer darüber hinaus ein Administrationsportal zur Verfügung.



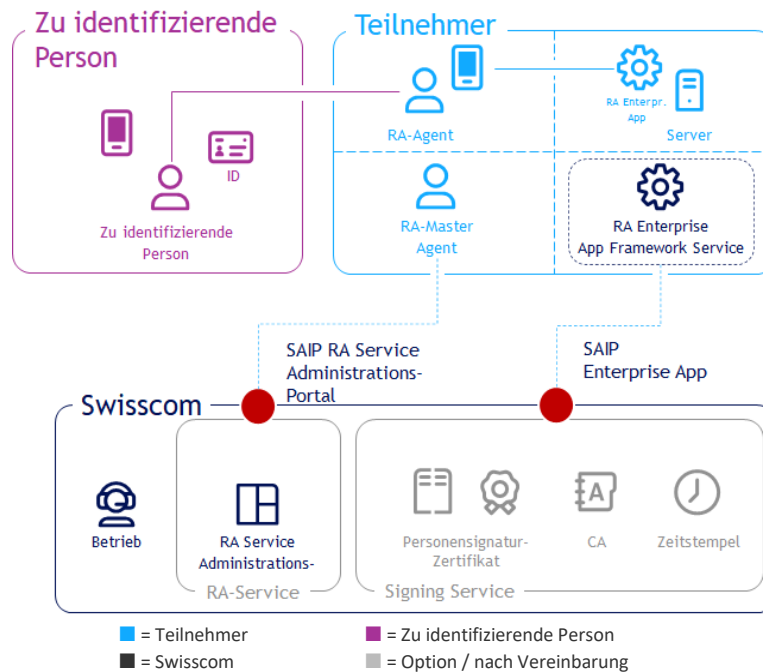
Auf der Grundlage eines separat abzuschliessenden RA Delegationsvertrags für die RA Enterprise App verpflichtet sich der Teilnehmer Swisscom gegenüber, während der Nutzung des zur Verfügung gestellten Frameworks die Personenidentifizierung entsprechend der Prozessvorgaben von Swisscom durchzuführen und die aufgenommenen Daten der Registrierungsstelle bei Swisscom zu übertragen. In der Funktion als Registrierungsstelle von Swisscom bestimmt der Teilnehmer hierzu einen sogenannten RA-Master-Agenten. Dieser wird einmalig von Swisscom geschult und kann danach weitere Mitarbeiter des Teilnehmers, somit der Registrierungsstelle, identifizieren und zum RA Agenten ernennen oder weitere RA-Master Agenten bestimmen. Jeder ernannte RA Agent durchläuft zunächst eine e-Learning Schulung und wird über seine Nutzungs- und Vertraulichkeitspflichten belehrt, damit er die Identifizierung einer Person in der Weise durchführt, dass anschliessend eine relevante Auswahl der Identifizierungsdaten auch für Signaturzwecke durch Swisscom genutzt werden können.

3 Definitionen

3.1 Service Access Interface Point (SAIP)

Der Service Access Interface Point (SAIP) ist der vertraglich vereinbarte, geografische und/oder logische Punkt, an dem ein Service dem Teilnehmer als Leistungsbezüger bereitgestellt, überwacht und die erbrachten Service Level ausgewiesen werden.

Folgende rein schematische Darstellung dient der Veranschaulichung der Leistungen und Leistungs-Komponenten des Framework Service:



Der Teilnehmer (Registrierungsstelle gemäss RA Delegationsvertrag für die RA Enterprise App) integriert das Framework in seine Applikation, die Enterprise App. Der Übergabepunkt (SAIP) ist die Schnittstelle zwischen dem Framework und dem teilnehmerspezifischen Teil der Applikation auf dem Mobilgerät. Ein weiterer Übergabepunkt (SAIP) ist der Zugang zum Swisscom Administrationsportal durch den vom Teilnehmer ernannten RA Master Agenten. Die Verfügbarkeit des Services ist dann gegeben, wenn Anfragen durch den Service entgegengenommen werden und entsprechend der Schnittstellenbeschreibung zum SAIP korrekt beantwortet werden. Die korrekte Antwort kann auch in einer dokumentierten oder für den Teilnehmer aussagekräftigen Fehlermeldung bestehen.

3.2 Servicespezifische Definitionen

Begriff	Beschreibung
eIDAS-Vo	EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt.
Enterprise App	Vom Teilnehmer oder in seinem Auftrag entwickelte, meist teilnehmerspezifischer Applikation, in der der Framework Service integriert wurde.
Evidenz	Beweis in Form eines signierten PDF Dokumentes. Dieses PDF enthält die Fotos und Scans die während dem Identifizierungsprozess erstellt wurden sowie die erhobenen Daten. Die Evidenz ist mit der elektronischen Signatur des RA Agenten versehen, der die Identifizierung durchgeführt hat.
Fortgeschrittene und qualifizierte elektronische Signatur	Die fortgeschrittene elektronische Signatur und die qualifizierte elektronische Signatur sind elektronische Signaturen, die der Signing Service zur Verfügung stellt.
Framework Service	Dienstleistung, die das Framework zur Verfügung stellt und den Softwarestand laufend aktuell hält.
Identifizierte Person	Siehe «zu identifizierende Person»
Mobile ID	Managed Service für die sichere Benutzer-Authentisierung. Mobile ID kann von verschiedenen Schweizer Providern, unter anderem Swisscom (Schweiz) AG, bezogen werden.



Begriff	Beschreibung
MRZ	"Machine Readable Zone", Teil eines Ausweis- oder Reisedokumentes, das mittels optischer Texterkennung gelesen werden kann.
Nutzungsbestimmungen	Die Nutzungsbestimmungen regeln im Verhältnis zwischen Swisscom (Schweiz) AG bzw. 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://trustservices.swisscom.com/repository/ abrufbar.
OCR	Automatisierte Texterkennung in Fotos.
OTP	One Time Password – Password, welches für eine einmalige Nutzung erzeugt und über SMS übertragen wird.
PWD	Password (-Eingabe), für die Authentisierung am Service.
RA Agent	Autorisierter Bediener der RA-App oder Enterprise App.
RA App	Applikation von Swisscom (Schweiz) AG unter Android und iOS, die eine Identifizierung und Registrierung ermöglicht und die gleichen Funktionalitäten wie die Enterprise App bietet.
RA Delegationsvertrag	Vertrag zur Delegation der Registrierungsstellentätigkeit, die der Teilnehmer dieses Service vorgängig zur Nutzung unterzeichnen muss.
RA Master Agent	Autorisierter Bediener der RA App und des RA Administrations Tool mit der Möglichkeit weitere RA Agenten oder Master RA Agenten für seine Organisation zu ernennen und zu verwalten.
RA-Service	Teil des Signing Service zur Entgegennahme und Archivierung der Identifizierungs- und Registrierungsdaten. Der Betrieb erfolgt in Zusammenhang mit der RA App oder einer Enterprise App oder über eine Import Schnittstelle.
Registrierung	Regulierter Prozess zur Ermittlung und Speicherung von Identifizierungsdaten sowie mit diesen Identifizierungsdaten verbundenen Authentisierungsmittel, die für die Auslösung einer elektronischen Signatur via Signing Service erforderlich sind.
Registrierungsstelle (RA)	Registrierungsstelle (Registration Authority) Zuständige Stelle für die Identifizierung der Signierenden. Teile des Prozesses der Registrierungsstelle können im Rahmen eines RA Delegationsvertrages durch Swisscom an Dritte ausgelagert werden.
SSL/TLS	Secure Socket Layer, Transport Layer Security, Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet basierend auf SSL (Zugangs-) Zertifikaten.
Teilnehmer	Der Teilnehmer ist entweder direkt Kunde von Swisscom mit einem kommerziellen Service Vertrag oder er hat einen kommerziellen Vertrag mit einem Reseller von Swisscom Services.
Teilnehmerapplikation	Der Teilnehmer gibt den Personen Zugang zu einer Applikation, mit der sie sich registrieren können oder elektronische Signaturen gemäss den Nutzungsbestimmungen von Swisscom erstellen können und der Teilnehmer stellt dabei neben der Authentisierung die Übertragung der Signaturdaten und Registrierungsdaten zum Fernsignaturservice von Swisscom sicher. Im Kontext dieser Leistungsbeschreibung stellt der Teilnehmer nur die RA Framework App.
ZertES	Schweizerisches Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate
Zu identifizierende Person, identifizierte Person	Natürliche Person, die bei vorgängiger Identifizierung, Authentifikation und Willensbekundung später ein Dokument elektronisch signieren möchte.

4 Ausprägungen und Optionen

Standardausprägung	RA Enterprise App Framework Service
Framework	●
e-Learning	●
Administrationsportal	●



Standardausprägung	RA Enterprise App Framework Service
Security Assessment (einmal jährlich maximal)	●
Beratung zu Erstellung Umsetzungskonzept, Security Assessment, Entwicklung	○

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

4.1 Definition der Leistungsausprägungen und Optionen

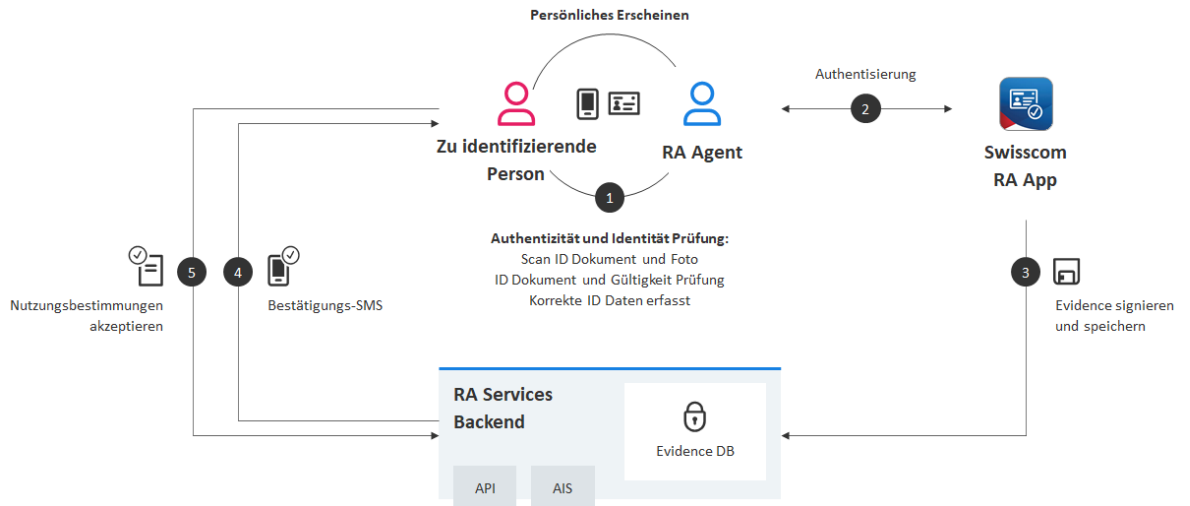
Leistungsausprägung/ Option	Definition
Framework	Binärcodesoftware, welche die von Swisscom vorgegebenen Identifikations- und Registrierungsprozesse abbildet und in die Framework App eingebunden wird. Es stellt die ermittelten Identifizierungsdaten dem Teilnehmer zur weiteren Verarbeitung zur Verfügung. Zusätzlich ermöglicht es die Übertragung der Evidenzen an den Signaturservice von Swisscom zur Registrierung für Signaturzwecke, was in einem separaten RA-Delegationsvertrag geregelt wird.
e-Learning	e-Learning Portal, auf dem ein als RA Agent benannter Nutzer des Teilnehmers eine Schulung durchlaufen kann, die ihn befähigt, Identifizierungen zum Zwecke der Übertragung an den Signaturservice von Swisscom durchzuführen. Hierzu muss er nach der Schulung einen Test erfolgreich abschliessen und kann erst dann als RA Agent auf den Frameworkteil der Enterprise App zugreifen. Teilnehmerspezifische Inhalte der Enterprise App ausserhalb der Funktionalität des Frameworks sind nicht Bestandteil des e-Learning und müssen vom Teilnehmer in einer eigenen Schulung sichergestellt werden.
Administrationsportal	Web-basierte Applikation für autorisierte Master RA Agenten zur Verwaltung des eigenen RA Agenten Netzwerks.
Security Assessment	Bei der Erstentwicklung und bei jeder Änderung der Enterprise App ist vor Inbetriebnahme der neuen oder geänderten Version ein Security Assessment notwendig. Dieses ist einmal jährlich im Servicepreis inkludiert.
Beratung zu Erstellung Umsetzungskonzept, Security Assessment, Entwicklung	Swisscom bietet Unterstützung bei der Erarbeitung des Umsetzungskonzeptes und der Auswahl geeigneter Softwarefirmen, die für die Entwicklung der Enterprise App oder die Durchführung des weiterer Security Assessments in Frage kommen könnten. Diese Leistung wird nach Zeit und Aufwand verrechnet.

4.2 Ablauf der Identifizierung und Registration

4.2.1 Prozessbeschreibung Identifizierung und Registration

Bei der Durchführung des Identifizierungs- und Registrierungsprozesses handelt der Teilnehmer in einer doppelten Rolle: einerseits identifiziert er die zu identifizierenden Personen für seine eigenen Zwecke und in eigenem Namen, andererseits handelt der Teilnehmer gleichzeitig als Registrierungsstelle für den Zertifizierungs- und Vertrauensdienst von Swisscom. Die Enterprise App nutzt zunächst den vom Framework zur Verfügung gestellten Identifikations- und Registrierungsprozess, der unverändert vom Teilnehmer zu übernehmen ist. Dieser Prozess setzt die Anforderungen um, welche Swisscom als Zertifizierungdienstanbieterin zu erfüllen hat. Der Service erlaubt es dem Teilnehmer, zusätzlich auch weitere Daten zu erheben, die nicht in der oben beschriebenen Doppelrolle erhoben werden, sondern nur dem Teilnehmer dienen und deshalb auch nicht an Swisscom für deren Zertifizierungsdienst übermittelt werden.

Der nachfolgende Prozessbeschrieb betrifft nur diejenigen Daten, die der Teilnehmer in seiner Doppelrolle auch als Registrierungsstelle von Swisscom mit dem vorgegebenen Identifizierungs- und Registrierungsprozess erhebt – zusätzliche Prozesse zur Datengewinnung nur für den Teilnehmer sind in teilnehmerindividuellen Vertragsdokumenten (insbesondere dem Umsetzungskonzept) geregelt:



- Der Teilnehmer bestimmt einen Master RA Agenten innerhalb seiner rechtlichen Einheit, welcher Personen innerhalb derselben Einheit identifizieren und diese als RA Agenten benennen kann. Die RA Agenten können sich nach erfolgreichem e-Learning an der Enterprise App authentisieren.
- Die Identifizierung durch andere Organisationen (z.B. Schwestergesellschaft, Externe) usw. benötigt aus datenschutzrechtlichen Gründen eine gesonderte Vereinbarung.
- Der Prozess setzt voraus, dass der RA Agent und die zu identifizierende Person sich an einem beliebigen Ort physisch treffen (1). Die zu identifizierende Person muss einen gültigen amtlichen Ausweis und ihr Mobiltelefon mitbringen.
- Der RA Agent authentisiert sich an der RA App über Mobile ID oder PWD/OTP (2).
- Nach der Authentisierung verlangt der RA Agent aus Datenschutzgründen die Zustimmung der zu identifizierenden Person zur Erhebung und Speicherung von Identitätsdaten und bestätigt dies in der App.
- Der RA Agent nimmt den Ausweis entgegen und wählt in der App die entsprechende Nationalität und den erlaubten Ausweistyp.
- In der App werden für die verschiedenen Nationalitäten und Ausweistypen jeweils Muster zum Vergleich angezeigt. Auf dem Muster werden auch optische oder haptische Sicherheits-Elemente markiert, die zur Echtheitsprüfung dienen.
- Der RA Agent prüft das Lichtbild auf dem Ausweis und stellt sicher, dass dieses ein Foto von der zu identifizierenden Person ist.
- Der RA Agent macht ein Foto von der Seite des Ausweisdokumentes, die keine MRZ enthält und löst anschliessend automatisch App gesteuert einen Scan der Seite aus, die eine MRZ enthält. Bei Pässen wird nur die MRZ Seite des Passes gescannt. Die MRZ wird durch einen OCR ausgelesen.
- Der RA Agent wird dann aufgefordert, ein Foto der zu identifizierenden Person mit Hintergrund der Umgebung zu machen (z.B. Tisch, charakteristische Wandbilder). Dieses Foto dient als Beweis für das persönliche Erscheinen während des Prozesses.
- Die ausgelesenen Daten (via OCR) werden dann in der App angezeigt, vom RA Agenten geprüft und allenfalls korrigiert, damit diese genau mit den Daten auf dem Ausweisdokument übereinstimmen.
- Nach Bestätigung der Identität bietet die App an, die Sprache der SMS-Kommunikation (deutsch, englisch, italienisch und französisch) für die identifizierte Person anzugeben. In dieser Sprache werden bei der zusätzlichen Übertragung der Identifizierungsdaten an den Signaturservice von Swisscom im Anschluss die Notifikationen und Nutzungsbestimmungen des Signaturservices in der gewählten Sprache via SMS ausgesendet.
- Der RA Agent wird jetzt aufgefordert, die Mobilnummer der identifizierten Person einzugeben und mittels eines Anrufes auf diese Nummer zu prüfen, ob die Person auch im Besitz dieser Nummer ist.
- Falls die Nummer korrekt ist, kann der RA Agent dann die Registrierung abschliessen, indem er sie mit seiner elektronischen Signatur bestätigt. (3)
- Der vom RA Agenten signierte Evidenz wird, durch die vom Teilnehmer bereitgestellten Funktionen der Enterprise App weiter für seine eigenen Zwecke verwertet. Der Teilnehmer kann den Datensatz auch mit weiteren Identifizierungsdaten anreichern, die er im Rahmen der Enterprise App selber ausserhalb des Frameworks bestimmt. Hierbei muss der Teilnehmer sicherstellen, dass die zu identifizierende Person hierfür vorgängig Teilnehmer-Nutzungsbestimmungen mit transparenten Regeln zum Datenschutz akzeptiert.
- Eine Kopie des für den Signing Service von Swisscom relevanten, signierten Datensatzes, wird nun als Evidenz an den Signing Service von Swisscom übertragen.
- Swisscom sendet daraufhin eine SMS mit einer URL zu den Nutzungsbestimmungen an die identifizierte Person.
- Für ihren Zertifizierungsdienst von Swisscom muss die identifizierte Person nun noch die Nutzungsbestimmungen bestätigen, indem er den Link in einer zugesandten SMS anklickt und die dort angezeigten Nutzungsbestimmungen



bestätigt. Die registrierte Person wird damit „Community Member“ der Swisscom Signierenden und kann für die Dauer der Gültigkeit der Identifizierung bei allen Signing Service-Teilnehmern der Swisscom eine elektronische Signatur erstellen lassen, ohne dass eine erneute Identifizierung notwendig ist, solange dies von der jeweiligen Teilnehmerapplikation zugelassen wird. Die Gültigkeitsdauer für die Erstellung einer QES ist auf die Gültigkeit des Ausweisdokumentes oder längstens 5 Jahre terminiert.

- Für ihren Zertifizierungsdienst wartet Swisscom die Annahme der Nutzungsbestimmungen durch die identifizierte Person ab und löscht die Identifizierungsdaten gemäss Datenschutzvorgaben, falls die identifizierte Person die Nutzungsbestimmungen abgelehnt hat oder spätestens nach 15 Tagen ohne Antwort der Person.
- Die Enterprise App-spezifischen Nutzungsbestimmungen sind vom Teilnehmer in einem gesonderten Dokument zu verfassen und zu verwalten. Im Umsetzungskonzept ist zu beschreiben, welche weiteren Daten für welchen Zweck erhoben werden und wie diese Erhebung so in den Enterprise App spezifischen Nutzungsbestimmungen abgebildet wird, so dass für die zu identifizierende Person insbesondere klar ist, welche Daten im Identifizierungs- und Registrierungsprozess für welche Zwecke erhoben werden (Evidenz einerseits für den Teilnehmer, andererseits für Swisscom, eventuell zusätzliche Daten nur für Zwecke des Teilnehmers).

4.2.2 Webportal für RA-Master Agenten

RA Master Agenten haben die Möglichkeit, verschiedene Administrationsaufgaben über ein von Swisscom zur Verfügung gestelltes Webportal durchzuführen:

- Ernennung von identifizierten und registrierten Personen der eigenen Organisation als RA-Agenten
- Verwaltung der RA Agenten (Informationen zur Identifikation und zum Authentisierungsmittel, Möglichkeit zur Löschung)
- Übersicht der von den RA-Agenten der eigenen Organisation identifizierten Personen anhand der Mobilnummer, die zur Authentisierung hinterlegt wurde:
 - Ansicht der Signaturmöglichkeiten (fortgeschritten/qualifiziert, EU/Schweiz), sogenannter «Level of Assurance (LOA)»
 - Ansicht des Ablaufes der Gültigkeit der Identifikation
 - Identifizierungsdatum
 - Vor- und Nachname
 - Land
 - Gültigkeit: global nutzbar oder nur im Kontext mit einem bestimmten Zugang einer Signaturapplikation
- Deaktivierung des Signierenden, d.h. Archivierung des Datensatzes

The screenshot shows the 'Users' page in the Swisscom RA Master Agent portal. At the top, there is a search bar with the value '079:'. Below it, the user profile for 'ING' is displayed, including a 'Register as agent' button. The profile shows the 'Level of Assurance ZertES' and 'eIDAS' sections, each with four green bars representing different levels of assurance, all with an expiration date of 25.07.2023. Below the profile is a table of evidence IDs.

Evidence Id	Created date	Serial Mobile Number	First Name	Last Name	Country Code	Validity	ID Expiry	LOA ZertES	LOA eIDAS	Status
5ca: [redacted]	02.04. [redacted]	MIDCHE4 [redacted]	ING [redacted]	[redacted]	DEU	global	[redacted] 23	4 (QCP)	4 (QCP)	Confirmed & Signed

Der Zugriff auf das Portal unter <https://ras-admin.scapp.swisscom.com> erfolgt unter Eingabe der MobileID und dem sogenannten Tenant (Datenbereich) der Organisation. Dieser wird dem Teilnehmer bei der Aufschaltung mitgeteilt.

4.2.3 Schnittstellen des Framework Service

Datenschnittstelle: Mit dem Framework werden im Prozess gemäss Ziff. 4.2.1 folgende Daten erhoben und im flüchtigen Speicher der Enterprise App dem Teilnehmer zur Verfügung gestellt:



- Mobilnummer
- Name
- Vorname
- Sprache (2-Zeichen Iso Code)
- Nationalität (3-Zeichen ISO 3166 [ISO3166])
- Dokumenttyp (3-Zeichen Code PAS für pass, IDC für ID)
- Geburtsdatum (Format: DD.MM.YYYY)
- Ablaufdatum des Ausweises (Format: DD.MM.YYYY)
- Seriennummer des Ausweises
- Fotos des vorgelegten Ausweisdokumentes (ID: Vorder- und Rückseite, Pass: Hauptseite) und von der identifizierten Person.

Übertragungsschnittstelle für die Evidenzen: Die Informationen werden über das Internet und das Mobilfunknetz übertragen. Die Nutzung der Enterprise App durch den RA Agent oder die Nutzung des Administrationsportal setzt eine Authentifizierung voraus, basierend auf den Zugangsdaten, die der RA Agent oder Master RA Agent bei der Identifizierung definiert hat (SMS bzw. MobileID). Ein Leistungsversprechen für das Funktionieren des Internets oder des Netzwerkbetriebs des Roaming Partners ist hierbei ausgeschlossen.

4.2.4 Onboarding Prozess

Bei der Bestellung des Framework Service wird ein technischer Ansprechpartner genannt.

Nach Eingang und Prüfung des Service Vertrages durch Swisscom erhält der genannte Ansprechpartner Zugriff auf den Binärcode des Swisscom Frameworks, um diesen in die Enterprise App einzubauen.

Parallel wird das Umsetzungskonzept vom Teilnehmer erstellt und mit Swisscom abgestimmt. Das Umsetzungskonzept definiert unter anderem folgende Punkte, die vertraglich eingehalten werden müssen:

- Formale Aspekte, die die Zusammenarbeit mit Swisscom definieren und zu erstellende Dokumentation.
- Rollen und Verantwortliche in der Teilnehmerorganisation.
- Prozessuale Aspekte, wie der Identifizierungsprozess, die Ernennung von Verantwortlichen, neue Versionen der Enterprise App.
- Die Anforderungen an das Security Assessment gemäss Ziff. 4.2.6.
- Datenschutzvorgaben und Vertraulichkeitsvorgaben und deren Einhaltung.

Swisscom sendet hierzu dem Teilnehmer eine Vorlage zu.

4.2.5 Freigabeprozess

Nach Fertigstellung der Enterprise App, informiert der Teilnehmer (Registrierungsstelle) Swisscom, dass die Enterprise App für das Security Assessment zur Verfügung steht. Swisscom führt das Security Assessment durch und meldet allfällige Abweichungen und Fehler mit der entsprechenden Kritikalität.

Die Freigabe für die Nutzung der Enterprise App erfolgt durch Swisscom, sofern:

- das Umsetzungskonzept freigegeben ist und
- das Security Assessment der App erfolgreich abgeschlossen ist.

Unter der Voraussetzung, dass der Teilnehmer einen separaten RA-Delegationsvertrag für die RA Enterprise App abgeschlossen hat, wird anschliessend ebenfalls durch Swisscom der erste Master RA Agent der Registrierungsstelle eingeschaltet.

4.2.6 Wesentliche Punkte des Security Assessments

Das Security Assessment untersucht folgende Sicherheitsanforderungen:

- Alle Evidenzdaten gemäss Ziffer 4.2.2, die vom RA Agenten aufgenommen wurden und in der Enterprise App dem RA Agenten angezeigt werden, werden (auch) an den RA Service der Swisscom übermittelt.
- Die im Umsetzungskonzept beschriebene Versionsnummer des Enterprise App Frameworks wird in der Enterprise App angezeigt.
- Die gelieferten Daten sind gemäss der Wertebereiche der Schnittstellenbeschreibung gültige Werte.
- Die Dateigrösse und Auflösung der Bilder werden bei der Übertragung nicht verändert.

4.2.7 Release Management

Planmässige Releases

- Swisscom informiert über den Kanal des technischen Ansprechpartners alle Teilnehmer, die den Framework Service einsetzen, über neue Releases.
- Swisscom wird in der Regel einmal im Jahr einen Major Release des Frameworks liefern.



- Der Teilnehmer ist verpflichtet, spätestens 12 Monaten nach einem Major Release die letzte Version des Frameworks in seiner Enterprise App zu integrieren und zu nutzen.
- Vor der produktiven Nutzung durch den Teilnehmer muss die Enterprise App mit dem Release durch den Swisscom beauftragen Compliance Officer per E-Mail oder schriftlich freigegeben werden.

Swisscom behält sich vor, die Einlieferung von Evidenzen in die Infrastruktur ihres Zertifizierungsdienstes zu unterbinden, sollten die Releases nicht rechtzeitig eingespielt sein.

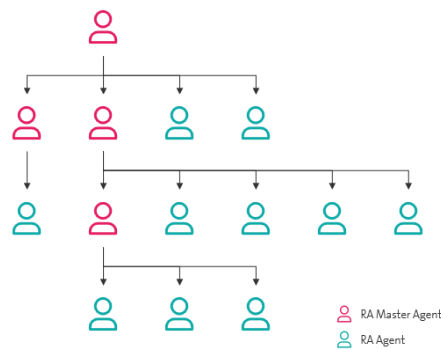
Behandlung von Security Patches

- Entscheidet Swisscom, dass aus Sicherheitsgründen ein Security Patch für das Framework eingespielt werden muss, wird folgender Prozess angewendet: Swisscom informiert über den Kanal des technischen Ansprechpartner alle Teilnehmer, die den Framework Service einsetzen, über die Änderung: Beschreibung des Problems, betroffene Version, Release Datum des Patches.
- Swisscom publiziert über denselben Kanal wie den Framework Service sämtliche Information, die benötigt werden, um den Security Patch einzupflegen.
- Der Teilnehmer integriert den Security Patch in seiner Enterprise App.
- Der Teilnehmer liefert ein Code Review, der beweist, dass keine andere Änderung in der Enterprise App eingeflossen sind.
- Der Swisscom beauftrage Compliance Officer gibt die Enterprise App per E-Mail frei.
- Der Teilnehmer sorgt für die rasche Verteilung der Enterprise App an seine Agenten innert maximal einem Monat.

Die Anwendung des Security Patch ist schnellstmöglich, In der Regel zwischen 2 und 6 Wochen umzusetzen. Swisscom behält sich vor, die Einlieferung von Evidenzen in die Infrastruktur ihres Zertifizierungsdienstes zu unterbinden, sollten die Security Patches nicht rechtzeitig eingespielt und die Enterprise App nicht abnehmbar gewesen sein.

4.3 Prozessbeschreibung RA Agenten Netzwerk und Schulungsprozess

Nach der Ernennung des ersten Master RA Agenten durch Swisscom, kann dieser nach entsprechender Authentisierung über ein von Swisscom zur Verfügung gestelltes, webbasiertes Administrationstool gemäss Ziffer 4.2.2 sein Netzwerk an RA Agenten aufbauen und weitere Master RA Agenten und RA Agenten ernennen. Hierbei werden zunächst Mitarbeiter des Teilnehmers identifiziert und dann als RA Agent oder RA Master Agent ernannt. RA Master Agenten können wiederum weitere RA Agenten benennen. Hierdurch kann der Teilnehmer ein komplettes Netzwerk von RA Master Agenten und RA Agenten selbstständig aufbauen:



Sobald ein RA Agent oder RA Master Agenten ernannt wird, bekommt dieser eine Aufforderung, die Schulung für RA Agenten durchzuführen. Diese Aufforderung erhält er per SMS-Notifikation, die einen Link zur e-Learning Plattform von Swisscom enthält, über die er selbstständig eine Schulung im Internet starten kann. Am Ende der Schulung absolviert der zukünftige Agent einen Test. Nach Bestehen des Tests bekommt der Agent noch eine SMS-Notifikation mit einem Link zu den Vertraulichkeits- und Mitwirkungspflichten. Erst nachdem diese akzeptiert wurden, kann der neue RA Agent Identifizierungen via Enterprise App durchführen.

4.4 Schulung und Sorgfalt bei der Identifizierung und Registration

RA Agenten und Master RA Agenten müssen für den Zugang zur Enterprise App eine e-Learning Schulung durchlaufen, sodass gewährleistet wird, dass die RA Agenten über geeignetes Wissen verfügen, um Identifizierungen durchzuführen. Der Teilnehmer ist über den RA Delegationsvertrag für Enterprise App zur Registrierungsstelle verpflichtet, die Mitarbeiter auf ihre Sorgfaltspflicht hinzuweisen. Jeder RA Agent wird auf seine Pflichten hingewiesen und signiert elektronisch bei erfolgreicher Schulung die Kenntnisnahme der Pflichten des RA Agenten, die Teil des RA Delegationsvertrages für die RA Enterprise App mit dem Teilnehmer sind.



Für die Schulung der Funktionalitäten ausserhalb der Funktionen des Frameworks ist der Teilnehmer selbst verantwortlich.

5 Leistungsdarstellung und Verantwortlichkeiten

Einmalige Leistungen

Tätigkeiten (S = STS/T = Teilnehmer)	S	T
Bereitstellung des Service		
1. Bereitstellung der Service Infrastruktur, allgemein RA Service für den Betrieb der Enterprise App: Hierzu gehört das Administrationsportal zur Verwaltung der registrierten Personen und zur Verwaltung der RA Agenten, das RA-Service Backend, sowie das e-Learning Modul.	✓	
2. Bereitstellung des Zugriffs auf das Swisscom Projekt "Framework Service" für die Erstellung der Enterprise App	✓	
3. Entwicklung der Enterprise App unter unverändertem Einbezug des Enterprise App Frameworks		✓
4. Bereitstellung eines Umsetzungskonzeptformulars mit den Punkten, die der Teilnehmer beschreiben muss	✓	
5. Erstellung des Umsetzungskonzepts und Einhaltung der im Rahmen des RA Delegationsvertrages für Enterprise App und Umsetzungskonzeptes benannten Auflagen		✓
6. Review des Umsetzungskonzepts und Rücksprache mit dem Teilnehmer	✓	
7. Zusenden des unterzeichneten RA Delegationsvertrages für die RA Enterprise App im Zusammenhang mit der Nutzung der Enterprise App und Nennung des ersten RA Master Agenten		✓
8. Bereitstellung der Enterprise App für das Security Assessment und die Abnahme durch Swisscom		✓
9. Security Assessment der Enterprise App vor Inbetriebnahme	✓	
10. Abnahme des Umsetzungskonzeptes	✓	
11. Abnahme der Enterprise App und Freigabe zur operationellen Nutzung	✓	
12. Schulung des ersten Master RA Agenten	✓	
13. Aufschaltung der Teilnehmerorganisation im RA Service und Eintrag des im RA Delegationsvertrag benannten RA Master Agenten des Teilnehmers	✓	
14. Bereitstellung eines Administrationsportals für den benannten RA Master Agenten des Teilnehmers zur Ernennung weiterer RA Agenten und RA Master Agenten	✓	
15. Bereitstellung des Zugangs zum e-Learning für die Identifizierungsaufgaben in der Enterprise App	✓	
16. Kontrolle des Zugangs zu den Funktionen der Enterprise App in Abhängigkeit vom e-Learning Status	✓	
17. Maintenance des Frameworks und Release Management	✓	
18. Bereitstellung und Sicherstellung der ordnungsgemässen Lizenzierung, für alle nicht Enterprise App Framework relevanten Teile der Enterprise App		✓
Beendigung des Service		
1. Meldung der Aufgabe der Geschäftstätigkeit sowie eine gegen den Teilnehmer gerichtete Konkursandrohung, die erfolgte Konkursöffnung oder eine Nachlassstundung		✓
2. Löschen der Berechtigungen und Zugänge sämtlicher RA Agenten und Master RA Agenten des Teilnehmers	✓	
3. Löschen des Administrationsbereiches für die Teilnehmerorganisation, der für die Organisation des Teilnehmers erstellt wurde («Tenant»)	✓	
4. Einstellung der Nutzung des Enterprise App Frameworks im Rahmen der Enterprise App		✓

Wiederkehrende Leistungen

Tätigkeiten (S = STS/T = Teilnehmer)	S	T
Standardleistungen		
1. Betrieb des Framework Service inkl. Schnittstellen, Administrationsportal und e-Learning Infrastruktur	✓	
2. Bereitstellung neuer Versionen des Enterprise App Frameworks (Releases, Security Patches)	✓	



Tätigkeiten (S = STS/T = Teilnehmer)	S	T
3. LifeCycle Management der Enterprise App (Schnittstellen Anpassungen, Integration neuer Versionen des Enterprise App Frameworks, Security Patches, zusätzliche Security Assessments)		✓
4. Anmeldung zu neuem Security Assessment und Freigabe der Enterprise App bei jedem neuen Release, der aufgrund von Anpassungen des Teilnehmers erfolgt		✓
5. Security Assessment der Enterprise App bei jedem neuen Release des Enterprise App Frameworks (maximal einmal jährlich)	✓	
6. Security Assessment der Enterprise App bei jedem weiterem neuen Release der Enterprise App		✓
7. LifeCycle Management der Infrastruktur des Teilnehmers: Anpassung an den aktuellen Stand der Technik und Sicherheit (Security Patches, Updates usw.) zum Schutz der Identifizierungsdaten		✓
8. Erstellen von Enterprise App spezifischen Nutzungsbestimmungen zur Regelung des Verhältnisses Teilnehmer – zu identifizierende Person (diese sollten insbesondere eine klare Regelung zum Datenschutz mit Abgrenzungen zur Datenerhebung für Swisscom enthalten) und Einholen der Akzeptanz der zu identifizierenden Person zu diesen Nutzungsbestimmungen		✓
9. Anpassung der Definition der Sicherheitsanforderungen	✓	
10. Sicherstellung des Einsatzes von technischen Authentifikationsmitteln und vertraglich vereinbarter Authentifizierungsmethoden (z.B. Mobile ID, PWD/OTP)		✓
11. Bereitstellung der Supportdienstleistungen (Service Desk, Incident Management usw.)	✓	
12. Melden von Mutationen der teilnehmerspezifischen Informationen (Kontaktpersonen, Organisationsbezeichnung usw.)		✓
13. Schulung der vom Teilnehmer ernannten RA Master Agenten zur Nutzung des Administrationstools und Sensibilisierung bezüglich regulatorischer Anforderungen	✓	
14. Sorgfalt bei der Auswahl von RA Agenten und deren Verwaltung (nur RA Agenten innerhalb der Organisation, Agenten löschen, wenn Sie die Organisation verlassen usw.)		✓
15. Schulung der RA Agenten durch das von Swisscom bereitgestellte e-Learning Verfahren	✓	
16. Melden von Sicherheitsvorfällen, die den RA Service betreffen		✓
17. Anpassung der Schnittstelle innerhalb der Enterprise App an geänderte Schnittstellen des Enterprise App Frameworks von Swisscom binnen von 12 Monaten		✓
18. Es werden nur Personen registriert, die nach bestem Wissen bzw. nach eigenen Angaben Ihren Wohnsitz in der Schweiz, dem EWR oder der EU haben, sofern mit Swisscom nicht explizit anderweitig vertraglich geregelt.		✓

6 Service Level und -Reporting

6.1 Service Level

Die nachfolgenden Service Levels beziehen sich grundsätzlich auf die vereinbarte Monitored Operation Time. Definitionen der Begriffe (Operation Time, Monitored Operation Time, Support Time, Availability, Security und Continuity) sowie die Beschreibung des Messverfahrens und des Reportings ergeben sich aus dem Vertragsbestandteil „Basisdokument“.

Folgende Service Levels werden erbracht. Bei mehreren möglichen Service Levels pro Ausprägung erfolgt die Auswahl des Service Levels im Servicevertrag.

Service Level & Zielwerte	RA Enterprise App Framework Service	
	RA-Service Admin Portal	Enterprise App (Framework)
Operation Time		



Service Level & Zielwerte			RA Enterprise App Framework Service	
			RA-Service Admin Portal	Enterprise App (Framework)
Monitored 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 ¹	Mo-Fr	08:00-17:00 ²	●	●
Störungsannahme	Mo-So	00:00-24:00	●	—
Availability				
Service Availability				
Schnittstelle zum RA Service	99.5%		●	—
Security				
Siehe Basisdokument			●	●
Continuity				
Service Continuity (STSSC)	RTO Best Effort RPO Best Effort		●	●

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

6.2 Service Level Reporting

Der RA Master Agent kann sich über das Administrationstool jederzeit über den Zustand des Service und über seine vorgenommenen und vom Service bearbeiteten Aktivitäten informieren.

7 Rechnungsstellung und Mengenreport

7.1 Rechnungsstellung

Die Rechnungsstellung erfolgt jeweils jährlich im Voraus. Verrechnet werden ausschliesslich Service Kosten für den Betrieb des Enterprise App Framework gemäss der aktuellen Preisliste. Die Rechnung ist fällig ab Einrichtung des Service für den Teilnehmer und Aufschaltung seines ersten Master RA Agenten.

Rechnungen für Consulting Dienstleistungen werden separat je nach Aufwand auf Basis der aktuellen Preislisten verrechnet.

7.2 Mengenreport

Es werden keine Reports erstellt.

¹ Wurde der Framework 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»



8 Besondere Regelungen

8.1 Bereitstellung des Frameworks durch Swisscom

Das Framework wird mit geschütztem Zugang auf einer Swisscom Plattform zur Verfügung gestellt. Neue Versionen werden nach vorheriger Ankündigung ebenfalls auf der Plattform veröffentlicht. Die Zugriffsdaten werden nach Abschluss des Vertrages an die im Servicevertrag genannte, technische Kontaktperson übermittelt. Die Kontaktperson darf die Zugriffsdaten keiner anderen Person offenlegen oder weitergeben. Der Zugriff ist für die Gesamtdauer des Vertrages gewährt. Der Wechsel der Kontaktperson ist Swisscom schriftlich anzuzeigen.

8.2 Anpassung Regulatorische Änderungen

Bei neuen oder angepassten regulatorischen oder gesetzlichen Anforderungen ist Swisscom eventuell gezwungen, am Enterprise App Framework oder an den in dieser Leistungsbeschreibung beschriebenen Prozessen Anpassungen vorzunehmen. Der Teilnehmer ist verpflichtet, diese Anpassungen ebenfalls vor dem Inkrafttreten der Änderung umzusetzen. Bei Nichteinhaltung dieser Bestimmung kann Swisscom die Nutzung des RA Enterprise Frameworks durch den Teilnehmer einschränken oder verhindern, indem sie die RA Agenten löscht und dem Teilnehmer im RA Service die Rechte entzieht. Ein solcher Eingriff von Swisscom stellt keine Vertragsverletzung dar.

8.3 Identifikation von Personen mit Wohnsitz ausserhalb EU/EWR/Schweiz

Der RA Service und die Swisscom Trust Services richten sich an Personen mit Wohnsitz in der EU, dem EWR und der Schweiz, da für Personen mit Wohnsitz ausserhalb dieser Regionen häufig andere rechtliche Bestimmungen (z.B. Konsumentenschutz und Datenschutzrecht) gelten. Es ist optional möglich, Registrierungen auch für Personen ausserhalb der EU, dem EWR und der Schweiz zuzulassen. Hierfür muss diese Möglichkeit explizit optional bestellt werden. Es werden dann die rechtlichen Möglichkeiten geprüft und ggfs. die Nutzungsbestimmungen oder andere Bestimmungen angepasst.