



As a leading trust service provider in Europe, we enable the most innovative digital business models .

Service Description

RA Enterprise App Framework Service

Swisscom Trust Services

Swisscom Trust Services AG

Konradstrasse 12
8005 Zürich

Switzerland

<https://trustservices.swisscom.com>

E-Mail: sts.salessupport@swisscom.com



1 Content

1	Content	2
2	Service overview	3
3	Definitions.....	4
3.1	Service Access Interface Point (SAIP).....	4
3.2	Service-specific definitions	4
4	Variants and options.....	5
4.1	Definition of the service specifications and options.....	6
4.2	Identification and registration process.....	6
4.2.1	Process description of the identification and registration	6
4.2.2	Portal for RA Master Agents.....	8
4.2.3	Interfaces of the Framework Service	8
4.2.4	Onboarding process	9
4.2.5	Release process.....	9
4.2.6	Essential aspects of the security assessment	9
4.2.7	Release management.....	9
4.3	Service description for the RA Agent network and training process	10
4.4	Training and due diligence when performing identifications and registrations.....	10
5	Service provision and responsibilities.....	11
6	Service levels and reporting.....	12
6.1	Service Levels.....	12
6.2	Service Level Reporting	13
7	Billing and quantity report.....	13
7.1	Billing	13
7.2	Quantity report.....	13
8	Special provisions.....	14
8.1	Provision of the Framework by Swisscom	14
8.2	Modification due to regulatory changes	14
8.3	Identification of persons domiciled outside the EU/EEA/Switzerland	14



2 Service overview

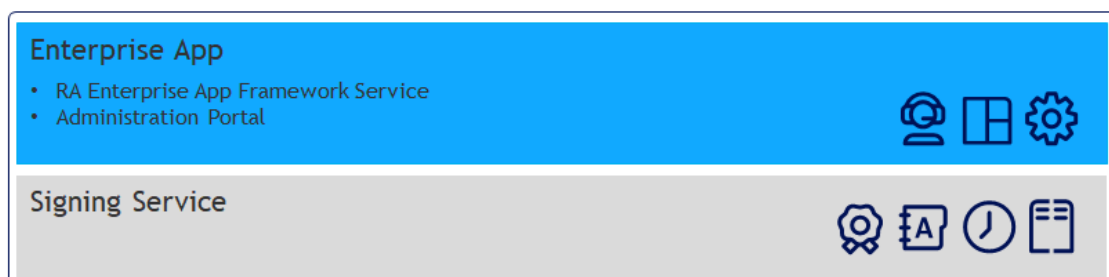
The signing service according to this service description is a server-based remote signature service of Swisscom IT Services Finance S.E., Vienna (AT), hereinafter referred to as "Swisscom ITSF" and Swisscom (Schweiz) AG. The signing service of Swisscom IT Services Finance S.E. will be provided in the data centers of Swisscom (Schweiz) AG in Switzerland and Swisscom Trust Services AG (hereinafter referred to as "Swisscom") distributes the Signing Service of both - Swisscom (Schweiz) AG for Switzerland and Swisscom IT Services Finance S.E. for the EU - in its own name or grants third parties the right to distribute the signing service in its own name.

The service is made available to Subscribers operating a subscriber application, the RA Enterprise App. The service for providing an RA Enterprise App Framework Service from Swisscom (hereinafter referred to as the "**Framework Service**") enables Subscribers to create their own applications and processes to register natural persons for the signing service. The Framework Service is provided by Swisscom (Switzerland) Ltd. and is part of Swisscom Trust Services. Registrations can be used for both advanced and qualified signatures in the EU and Switzerland.

Specifically, the Framework Service enables the Subscriber to develop its own application for mobile devices (hereinafter referred to as the "**Enterprise App**"), which it then uses to establish business relationships with natural persons (hereinafter referred to as "persons to be identified" or "identified persons" after registration) when in contact face to face.

The Enterprise App must be created by the Subscriber itself or its subcontracted third party. Important identification functions are provided by Swisscom within the scope of an **Enterprise App Framework** (hereinafter referred to as the "**Framework**"). The registration requirements based on the Framework are mapped in the Enterprise App in such a way that the registration data — based on a separate **RA delegation contract for the RA Enterprise App** — is simultaneously collected by the Subscriber (in its capacity as a Registration Authority) for Swisscom (in its capacity as the provider of certification services) and made available to Swisscom's certification service and Trust Service. Based on the registration process and the registration data, Swisscom may offer its electronic signature service to the Registered Person without the Registered Person having to undergo the same registration process a second time.

The Enterprise App is provided within the scope of a service that ensures ongoing monitoring of the functionality and ongoing troubleshooting as well as function updates. In addition, an administration portal is available to the Subscriber, where it can check the data used for the signature.



On the basis of a separate RA delegation contract for the RA Enterprise App, the Subscriber promises Swisscom that, when using the Framework provided, it will perform personal identifications in accordance with Swisscom's process specifications and transfer any data recorded to Swisscom's Registration Authority. In its capacity as Swisscom's Registration Authority, the Subscriber shall appoint a Master RA Agent for this purpose. This person will be trained once by Swisscom, after which he/she may identify additional employees of the Subscriber, i.e. Registration Authority, and appoint them as RA Agents or additional Master RA Agents. Each appointed RA Agent first undergoes an e-learning training course and is instructed on his/her usage and confidentiality obligations, so that he/she can identify a person in such a way that a relevant selection of identification data can then also be used by Swisscom for signature-related purposes.

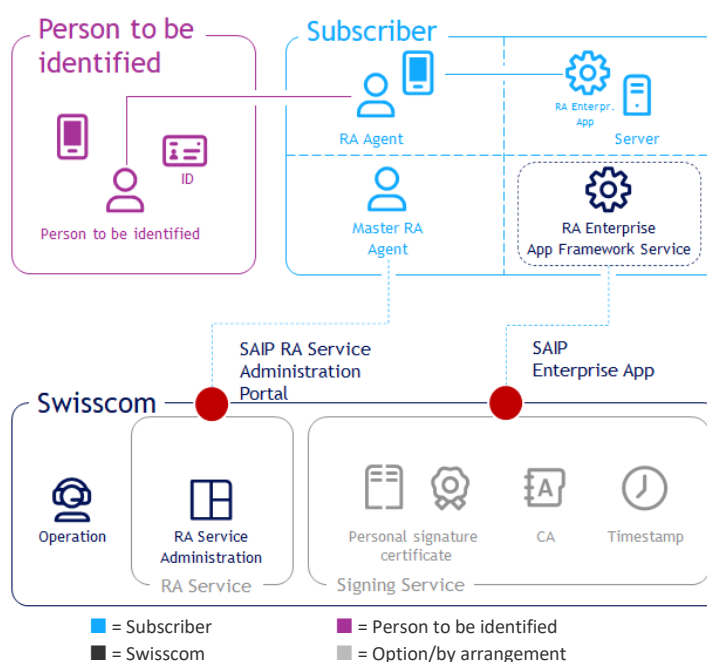


3 Definitions

3.1 Service Access Interface Point (SAIP)

The Service Access Interface Point (SAIP) is the contractually agreed, geographical and/or logical point at which a service is delivered to the Subscriber as service user. It is also the point at which a service is monitored and the service level provided is documented.

The following purely schematic diagram serves to demonstrate the services and service components of the Framework Service:



The Subscriber (Registration Authority in accordance with the RA delegation contract for the RA Enterprise App) integrates the Framework into its application, the Enterprise App. The service access interface point (SAIP) is the interface between the Framework and the Subscriber-specific part of the application on the mobile device. Another service access interface point (SAIP) is the access point to the Swisscom administration portal used by the Subscriber-appointed Master RA Agent. The availability of this service is assured if enquiries are accepted by the Service and answered correctly to the SAIP in line with the interface description. The correct reply can also consist of an error message that is documented or meaningful for the Subscriber.

3.2 Service-specific definitions

Term	Description
Advanced and qualified electronic signature	Advanced and qualified electronic signatures are electronic signatures provided by the Signing Service.
eIDAS regulation	EU Regulation on electronic identification and trust services for electronic transactions in the internal market.
Enterprise App	Subscriber-developed or developed by Subscriber's subcontractor, mostly Subscriber-specific application which the Framework Service was integrated into.
Evidence	Evidence in the form of a signed PDF document. This PDF contains the photos and scans created during the identification process, as well as any data collected. The electronic signature of the RA Agent who carried out the identification is attached to the evidence.
Framework Service	A service provided by the Framework that keeps the software up-to-date on an ongoing basis.
Identified person	See "person to be identified"
Master RA Agent	Authorised operator of the RA App and RA Administration Tool, who is able to appoint and manage additional RA Agents and Master RA Agents for his/her organisation.



Term	Description
Mobile ID	Managed service for secure user authentication. Mobile ID can be purchased from various Swiss providers, including Swisscom (Switzerland) Ltd..
MRZ	"Machine Readable Zone", part of a passport or travel document that can be read using optical text recognition.
OCR	Automated text recognition in photos.
OTP	One Time Password – password created for use on one occasion which is sent via SMS.
Person to be identified, identified person	Natural person who wants to sign a document electronically after prior identification, authentication, and declaration of consent.
PWD	Password (entry) for the authentication of the password to be used for the service.
RA Agent	Authorised operator of the RA App or Enterprise App.
RA App	Swisscom (Switzerland) Ltd. application on Android and iOS that enables identification and registration and offers the same functionalities as the Enterprise App.
RA delegation contract	Contract governing the delegation of the Registration Authority's activities, which the Subscriber must sign in advance in order to use this service.
RA service	Part of the Signing Service for receiving and archiving identification and registration data, which is operated in connection with the RA App or an Enterprise App or via an import interface.
Registration	Regulated process for identifying and storing identification data and the means of authentication associated with such identification data that are required to trigger an electronic signature via the Signing Service.
Registration Authority (RA)	Authority responsible for identifying the signatories. Under an RA delegation agreement, Swisscom may outsource parts of the registration process to third parties.
SSL/TLS	Secure socket layer, transport layer security, encryption protocol for secure data transmission on the internet based on SSL (access) certificates.
Subscriber	The subscriber is either a direct customer of Swisscom with a commercial service contract or has a commercial contract with a reseller of Swisscom services.
Subscriber application	The subscriber provides persons with access to an application with which they can register or create electronic signatures in accordance with Swisscom's terms and conditions of use, and the subscriber ensures not only the authentication but also the transmission of the signature data or the registration data to the remote signature service of Swisscom. In the context of this service description the subscriber application is the RA Enterprise App.
Terms and conditions of use	The terms and conditions of use govern the terms for using the signature certificates and signature service within the scope of the relationship between Swisscom (Switzerland) Ltd or Swisscom IT Services Finance S.E. and the signatory on a subscriber application. They can be viewed at https://trustservices.swisscom.com/repository/
ZertES	Federal Act of 19 December 2003 on Certification Services in relation to Electronic Signatures, commonly referred to as the Swiss Federal Act on Electronic Signatures (Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur or "ZertES")

4 Variants and options

Standard variant	RA Enterprise App Framework Service
Framework	●
e-learning	●
Administration portal	●
Security assessment (no more than once per year)	●



Standard variant	RA Enterprise App Framework Service
Advice on the creation of an implementation concept, security assessment, development	○

● = Standard (included in the price) ○ = For an additional fee

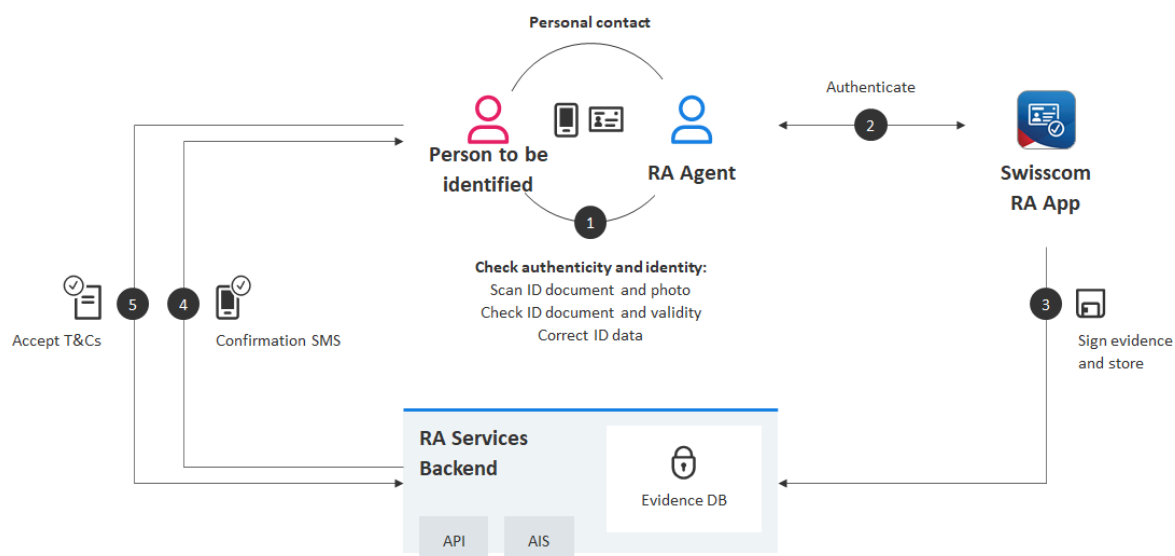
4.1 Definition of the service specifications and options

Specification/Option	Definition
Framework	Binary code that maps the identification and registration processes specified by Swisscom and can be implemented into the Framework App. It makes the identification data available to the Subscriber for further processing. It also enables evidence to be transferred to Swisscom's signature service in order to be registered for signature-related purposes; this is regulated in a separate RA delegation contract.
e-learning	e-learning portal where a user designated by the Subscriber as the RA Agent can undergo training that will enable him/her to perform identifications, which are then transferred to Swisscom's signature service. To do this, he/she must pass a test at the end of the training course, only after which will he/she be permitted to access the Framework portion of the Enterprise App as a RA Agent. The e-learning session does not cover any Subscriber-specific contents of the Enterprise App beyond the functionality of the Framework; this must be covered by the Subscriber within the scope of its own training.
Administration portal	Web-based application for authorised Master RA agents to manage their own RA Agent network.
Security assessment	A security assessment is required for the initial development and for every modification made to the Enterprise App before the new or modified version is put into service. One security assessment per year is included in the service charge.
Advice on the creation of an implementation concept, security assessment, development	Swisscom offers support on developing the implementation concept and selecting suitable software companies that could be considered for the development of the Enterprise App or for carrying out further security assessments. This service is invoiced according to time and effort.

4.2 Identification and registration process

4.2.1 Process description of the identification and registration

When carrying out the identification and registration process, the Subscriber plays a dual role: on the one hand, it identifies the person to be identified for its own purposes and in its own name; on the other hand, the Subscriber simultaneously acts as the Registration Authority for Swisscom's certification service. The Enterprise App initially uses the identification and registration process provided by the Framework, which must be adopted unchanged by the Subscriber. This process implements the requirements that Swisscom must meet as a provider of certification and trust services. The service also allows the Subscriber to collect additional data not otherwise collected within the scope of its dual role as described above, but only serves the Subscriber and is therefore not transmitted to Swisscom for use with its certification service. The following process description concerns only the data that the Subscriber collects as part of its dual role, whereby one aspect of this is to serve as Swisscom's registration authority, using the specified identification and registration process; additional processes aimed at collecting data only for the Subscriber's purposes are regulated in Subscriber-specific contract documents (in particular the implementation concept):



- The Subscriber shall designate a Master RA Agent within its legal entity, who can identify persons within the same entity and appoint them as RA Agents. The RA Agents can authenticate themselves using the Enterprise App following the successful completion of the e-learning course.
- For reasons related to data protection, identification by other organisations (e.g. affiliate, external) etc. requires a separate agreement.
- The process requires that the RA Agent and the person to be identified physically meet at any location (1). The person to be identified must bring a valid official ID and their mobile phone.
- The RA Agent authenticates himself/herself in the RA App using a Mobile ID or PWD/OTP (2).
- After authentication, the RA Agent asks the person to be identified to consent to the collection and storage of his/her identification data for data protection reasons and confirms this in the app.
- The RA Agent receives the ID and selects the appropriate nationality and the permitted ID type in the app.
- The app displays sample IDs for the different nationalities and ID types for comparison. The sample contains mark-ups showing visual or tactile security features that help verify the authenticity of the ID.
- The RA Agent checks the photo on the ID and makes sure that it is a photo of the person to be identified.
- The RA Agent takes a photo of the page of the ID document that does not contain an MRZ and then automatically triggers an app-controlled scan of the page with an MRZ. In the case of passports, only the MRZ side of the passport is scanned. The MRZ is read by an OCR.
- The RA Agent is then asked to take a photo of the person to be identified that includes their surroundings in the background (e.g. table, characteristic wall paintings). This photo serves as evidence that the person was physically present during the process.
- The data read out (via OCR) is then displayed in the app, checked by the RA Agent and, if necessary, corrected so that it exactly matches the data on the ID document.
- After confirming the person's identity, the app offers to specify their preferred language for communication via SMS (German, English, Italian or French). After the identification data is transmitted to Swisscom's signature service in that language, the notifications and terms of use of the signature service are also sent out via SMS in the selected language.
- The RA Agent is then asked to enter the mobile number of the person to be identified and to call it to check whether it is correct.
- If the number is correct, the RA Agent can complete the registration by affixing his/her electronic signature as confirmation. (3)
- The evidence signed by the RA Agent will be used for the Subscriber's own purposes by the Enterprise App functions provided by the Subscriber. The Subscriber can also enrich the data record even further by defining additional identification data to be collected by the Enterprise App, which extend beyond the Framework. Here, the Subscriber must ensure that the identified person first accepts the Subscriber's terms and conditions of use with transparent rules on data protection.
- A copy of the signed data record relevant for Swisscom's signing service is then transmitted to Swisscom's Signing Service as evidence.
- After this, Swisscom sends an SMS containing a URL to the terms and conditions of use to the identified person.
- To use the Swisscom certification service, the identified person still has to confirm the terms and conditions of use by clicking on the link in an SMS sent to them and confirming the terms and conditions of use shown there. The registered person thus becomes a member of the Swisscom signatory community, and can have a valid electronic



signature created for all subscribers to Swisscom's Signing Service for the duration of the period of validity of the identification without having to repeat the identification process, provided this is permitted by the subscriber application concerned. The period of validity when creating a QES is limited to the period of validity of the ID document or a maximum of 5 years.

- For its certification service, Swisscom waits for the identified person to accept the terms and conditions of use and, in accordance with data protection requirements, deletes all identification data if the identified person has rejected the terms and conditions of use or at the latest after 15 days without a reply from the identified person.
- The Subscriber must prepare and manage terms and conditions of use specific to the Enterprise App in a separate document. The implementation concept must describe which additional data is collected for which purpose and how this data is mapped in the Enterprise App-specific terms and conditions of use, so that the person to be identified understands clearly which data is collected during the identification and registration process and for which purposes (evidence for both the Subscriber and Swisscom, possibly additional data only for the Subscriber's purposes).

4.2.2 Portal for RA Master Agents

RA Master Agents have the possibility to perform various administration tasks via a web portal provided by Swisscom:

- Appointment of identified and registered persons of their own organisation as RA agents
- Management of RA agents (information on identification and authentication, possibility of deletion)
- Overview of the persons identified by the RA @-@ agents of their own organisation using the mobile number registered for authentication:
 - View of signature options (advanced/qualified, EU/Switzerland), so called "Level of Assurance (LOA)"
 - View of the expiry of the validity of the identification
 - Identification date
 - Surname and surname
 - Country
 - Validity: Globally usable or only in context with a specific access of your signature application
- Deactivate the identified and/or registered person (archive the data set)

The screenshot displays the Swisscom RA Master Agents portal. At the top, there is a navigation bar with the Swisscom logo, 'Agents', and 'Users' tabs. A user profile is shown as 'ING (Master RA Agent) Swis...'. Below the navigation bar, the 'Users' section is active, featuring a search bar with the text '079'. A user card for 'ING' is visible, showing a 'Register as agent' button and a 'Level of Assurance ZertES' section with four green bars representing different assurance levels. Below this, an 'eIDAS' section also shows four green bars. At the bottom, a table lists users with columns: Evidence Id, Created date, Serial Mobile Number, First Name, Last Name, Country Code, Validity, ID Expiry, LOA ZertES, LOA eIDAS, and Status. One user is listed with Evidence Id 5ca, Created date 02.04, Serial Mobile Number MIDCHE, First Name ING, Last Name, Country Code DEU, Validity global, ID Expiry 23, LOA ZertES 4 (QCP), LOA eIDAS 4 (QCP), and Status Confirmed & Signed.

Access to the portal under <https://ras-admin.scapp.swisscom.com> is done by entering the MobileID and the so-called tenant (data area) of the organisation. This will be communicated to the Subscriber at the time of setup.

4.2.3 Interfaces of the Framework Service

Data interface: Pursuant to Section 4.2.1, the Framework is used to collect the following data throughout the process and make it available to the Subscriber in the Enterprise App's volatile memory:



- Mobile number
- Surname
- First name
- Language (2-letter ISO code)
- Nationality (3-letter ISO 3166 [ISO3166])
- Document type (3-letter code; PAS for passport, IDC for ID)
- Date of birth (format: DD.MM.YYYY)
- ID expiration date (format: DD.MM.YYYY)
- Serial number on the ID
- Photos of the ID document presented (ID: front and back, passport: main page) and of the identified person itself

Transmission interface for evidences: The information is transmitted via the Internet and the mobile network. Use of the Enterprise App by the RA Agent or use of the administrative portal requires that the user is authenticated based on the access data defined by the RA Agent or Master RA Agent during identification (SMS or MobileID). A promise guaranteeing the functioning of the Internet or the operability of the roaming partner's network is excluded.

4.2.4 Onboarding process

A technical contact person is named when the Framework Service is ordered.

Once Swisscom has received and reviewed the service contract, the contact person named shall be given access to the binary code of the Swisscom Framework in order to integrate it into the Enterprise App.

At the same time, the implementation concept is drawn up by the Subscriber and coordinated with Swisscom. The implementation concept defines, among other things, the following points for which contractual compliance is mandatory:

- Formal aspects defining cooperation with Swisscom and the documentation to be prepared.
- Roles and responsibilities in the Subscriber's organisation.
- Process-related aspects, such as the identification process, the appointment of responsible persons, new versions of the Enterprise App.
- The requirements for the security assessment according to Section 4.2.6.
- Data protection and confidentiality requirements and their compliance.

Swisscom sends a template of the implementation concept to the Subscriber.

4.2.5 Release process

Once the Enterprise App has been completed, the Subscriber (registration authority) notifies Swisscom that the Enterprise App is ready for the security assessment. Swisscom carries out the security assessment and reports any deviations and errors and their respective severity level.

Swisscom will release the Enterprise App for use, if:

- the implementation concept has been released and
- the app's security assessment has been successfully completed.

Provided that the Subscriber has concluded a separate RA delegation contract for the RA Enterprise App, Swisscom will then also activate the first Master RA Agent of the registration authority.

4.2.6 Essential aspects of the security assessment

The security assessment examines the following security requirements:

- All evidence data as defined in Section 4.2.2, which is entered by the RA Agent and displayed to the RA Agent in the Enterprise App is (also) transmitted to Swisscom's RA service.
- The version number of the Enterprise App Framework described in the implementation concept is displayed in the Enterprise App.
- The data delivered are valid entries according to the ranges provided in the interface description.
- Neither the images' file size nor resolution change during transmission.

4.2.7 Release management

4.2.7.1 Scheduled releases

- Swisscom uses the technical contact as a channel to inform all Subscribers using the Framework Service about new releases.
- As a rule, Swisscom will deliver a major release of the Framework once a year.



- The Subscriber is obliged to integrate and use the latest version of the Framework in its Enterprise App no more than 12 months following a major release.
- Before the Enterprise App can be used productively by the Subscriber, it must be approved for release by Swisscom's Compliance Officer by e-mail or in writing.

Swisscom reserves the right to prevent the submission of evidence to the infrastructure of its certification service if the releases are not installed on time.

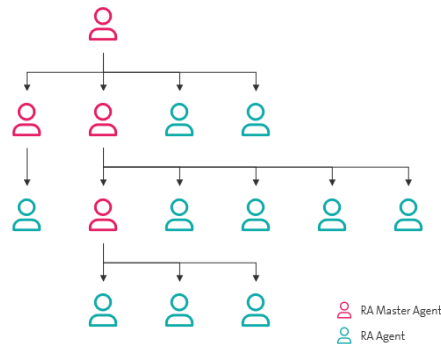
4.2.7.2 Handling security patches

- If Swisscom decides that a security patch must be installed on the Framework for security reasons, the process is as follows: Swisscom uses the technical contact as a channel to inform all Subscribers using the Framework Service about the modification: description of the problem, version affected, release date of the patch.
- Swisscom uses the same channel as for the Framework Service to publish all information required for integrating the security patch.
- The Subscriber integrates the security patch into its Enterprise App.
- The Subscriber provides a code review that proves that no other changes have been made to the Enterprise App.
- The Compliance Officer commissioned by Swisscom releases the Enterprise App by e-mail.
- The Subscriber ensures the rapid distribution of the Enterprise App to its agents within no more than one month.

The security patch must be applied for as quickly as possible, usually in 2 to 6 weeks. Swisscom reserves the right to prevent the submission of evidence to the infrastructure of its certification service if the security patches have not been installed on time and the Enterprise App could not be released.

4.3 Service description for the RA Agent network and training process

After the first Master RA Agent is appointed by Swisscom and has authenticated himself/herself in the system, the Master RA Agent will be able to set up his/her network of RA Agents and appoint additional Master RA Agents and RA Agents via a web-based administration tool provided by Swisscom according to section 4.2.2. During this process, the Subscriber's employees are identified first and then appointed as RA Agents or Master RA Agents. Master RA Agents can then name additional RA Agents, thereby enabling the Subscriber to independently create an entire network of Master RA Agents and RA Agents:



As soon as an RA Agent or Master RA Agent is appointed, that RA Agent or Master RA Agent receives an invitation to undergo RA Agent training. This request is sent via SMS and contains a link to Swisscom's e-learning platform, which the RA Agent or Master RA Agent can use to independently start taking a training course online. Once he/she has reached the end of the training course, the future agent takes a test. After passing the test, the agent receives an SMS notification containing a link to the confidentiality obligation and duties of cooperation. Only after these have been accepted can the new RA Agent perform identifications via the Enterprise App.

4.4 Training and due diligence when performing identifications and registrations

RA Agents and Master RA Agents must undergo an e-learning training course to access the Enterprise App in order to ensure that RA Agents have the knowledge they need to perform identifications. In accordance with the RA delegation contract for the Enterprise App, the Subscriber has an obligation vis-à-vis the registration authority to inform its employees of their duty of care. Each RA Agent is informed of his/her duties and, once he/she has successfully completed the training course, provides a digital signature in acknowledgement of the RA Agent's duties, which form part of the RA delegation contract with the Subscriber for the RA Enterprise App.

The Subscriber itself is responsible for providing training for any functionalities that extend beyond the Framework's standard functions.



5 Service provision and responsibilities

Non-recurring services

Activities (S = STS/Sb = Subscriber)	S	Sb
Provision of service		
1. Provision of the service infrastructure, general RA service for the operation of the Enterprise App: This includes the administrative portal for managing the registered persons, RA Agents, the RA service backend, as well as the e-learning module.	✓	
2. Provision of access to Swisscom's "Framework Service" project for the creation of the Enterprise App	✓	
3. Development of the Enterprise App with no changes with respect to the integration of the Enterprise App Framework		✓
4. Provision of an implementation concept form listing the points to be described by the Subscriber	✓	
5. Preparation of the implementation concept and compliance with the requirements specified in the RA delegation contract for the Enterprise App and the implementation concept		✓
6. Review of the implementation concept and consultation with the Subscriber	✓	
7. Sending the signed RA delegation contract for the RA Enterprise App in connection with the use of the Enterprise App and the appointment of the first Master RA Agent		✓
8. Provision of the Enterprise App for the security assessment and acceptance by Swisscom		✓
9. Security assessment of the Enterprise App before it is put into service	✓	
10. Acceptance of the implementation concept	✓	
11. Acceptance of the Enterprise App and release for operational use	✓	
12. Training of the first Master RA Agent	✓	
13. Activation of the Subscriber organisation in the RA service and entry of the Subscriber's Master RA Agent as designated in the RA delegation contract	✓	
14. Provision of an administrative portal for the Subscriber's designated Master RA Agent to appoint additional RA Agents and Master RA Agents	✓	
15. Provision of access to an e-learning course for identification tasks in the Enterprise App	✓	
16. Controls access to Enterprise App functions depending on a user's e-learning status	✓	
17. Framework maintenance and release management	✓	
18. Provision and assurance that licensing is being handled correctly for all parts of the Enterprise App that are not relevant to the Enterprise App Framework.		✓
Termination of the service		
1. Notification of the relinquishment of business activities, a bankruptcy notice against the Subscriber, the opening of bankruptcy proceedings or a debt restructuring moratorium		✓
2. Deletion of authorisations and access for all of the Subscriber's RA Agents and Master RA Agents	✓	
3. Deletion of the administrative area for the Subscriber organisation that was created for the Subscriber's organisation ("Tenant")	✓	
4. Termination of the use of the Enterprise App Framework within the scope of the Enterprise App		✓

Recurring services

Activities (S = STS/Sb = Subscriber)	S	Sb
Standard services		
1. Operation of the Framework Service incl. interfaces, administrative portal and e-learning infrastructure	✓	
2. Provision of new versions of the Enterprise App Framework (releases, security patches)	✓	
3. Lifecycle management of the Enterprise App (interface modifications, integration of new versions of the Enterprise App Framework, security patches, additional security assessments)		✓



Activities (S = STS/Sb = Subscriber)	S	Sb
4. Registration for a new security assessment and release of the Enterprise App, with each new release needed due to customisations		✓
5. Security assessment of the Enterprise App with every new release of the Enterprise App Framework (no more than once a year)	✓	
6. Security assessment of the Enterprise App with each new release of the Enterprise App		✓
7. Lifecycle management of the Subscriber's infrastructure: Updating to the current status of technology and security (security patches, updates etc.) for the protection of identification data		✓
8. Creation of Enterprise App-specific terms and conditions of use to regulate the relationship between the Subscriber and the Person to be identified (including, in particular, a clear rule governing data protection with limitations on data collection for Swisscom) and obtaining the identified person's acceptance of these terms and conditions of use		✓
9. Amendment of the definition of the security requirements	✓	
10. Ensuring the use of technical means of authentication and contractually agreed authentication methods (e.g. Mobile ID, PWD/OTP)		✓
11. Provision of support services (service desk, incident management, etc.)	✓	
12. Reporting of changes to Subscriber-specific information (contact persons, name of the organisation, etc.)		✓
13. Training of the Master RA Agents appointed by the Subscriber to use the administrative tool and rSigning Servicee their awareness of regulatory requirements	✓	
14. Careful selection and management of RA Agents (only RA Agents within the organisation, delete agents when they leave the organisation, etc.)		✓
15. RA Agent training by means of the e-learning process provided by Swisscom	✓	
16. Reporting security incidents that affect the RA service		✓
17. Adapting the interface within the Enterprise App to modified interfaces of Swisscom's Enterprise App Framework within 12 months		✓
18. Only persons who, to the best of the RA-Agent's knowledge or according to their own information, are resident in Switzerland, the EEA or the EU will be registered, unless otherwise explicitly contractually agreed with Swisscom.		✓

6 Service levels and reporting

6.1 Service Levels

The following service levels generally relate to the agreed monitored operation times. Definitions of terms (Operation Time, Monitored Operation Time, Support Time, Availability, Security and Continuity) and the description of the measurement method and reporting are set out in the contractual element "Base Document".

The following service levels are provided for the service variants (see section 3). If several possible service levels are available for each variant, the service level is selected in the service contract..

Service levels & target values	RA Enterprise App Framework Service	
	RA service Admin portal	Enterprise App (Framework)
Operation time		



Service levels & target values			RA Enterprise App Framework Service	
			RA service Admin portal	Enterprise App (Framework)
Monitored Operation Time	Mo-Su	00:00-24:00	●	—
Provider Maintenance Window	PMW DC	PMW Swisscom Data Centre	●	—
	PMW-S: With advance notice for security and system-critical updates	Daily 19:00-07:00, only for announced maintenance	●	—
Support Time				
Support Time ¹	Mo-Fr	08:00-17:00 ²	●	●
Fault Acceptance	Mo-Su	00:00-24:00	●	—
Availability				
Service Availability				
Interface to the RA service	99.5%		●	—
Security				
See base document			●	●
Continuity				
Service Continuity (STSSC) ³	RTO Best Effort RPO Best Effort		●	●

● = Standard (included in the price) ○ = For an additional charge — = Not available

6.2 Service Level Reporting

The Master RA Agent can use the administrative tool at any time to obtain information regarding the status of the service and any activities performed and processed by the service.

7 Billing and quantity report

7.1 Billing

Services are invoiced in advance on an annual basis. Only service costs incurred in connection with the operation of the Enterprise App Framework will be charged in accordance with the current price list. The invoice shall become due as soon as the service has been set up for the Subscriber and the Subscriber's first Master RA agent has been activated. Invoices for consulting services will be invoiced separately on a cost basis in accordance with the current price lists.

7.2 Quantity report

No reports are produced.

¹ If the Framework Service was purchased via a Swisscom partner, they should generally be contacted in the event of faults. If the partner is not able to rectify the fault, the partner will pass it on to Swisscom.

² Holidays: See "SLA Definitions" basic document

³ RTO and RPO only concern the provision of the Signing Service on SAIP. Mobile services used for the identification, authentication or declaration of consent are not included here.



8 Special provisions

8.1 Provision of the Framework by Swisscom

The Framework is provided with protected access on the Swisscom Repository. New versions will also be published on the repository platform following advance notice. The access data will be transmitted to the technical contact person named in the service contract following the conclusion of the contract. The contact person may not disclose nor pass on the access data to any other person. Access is granted for the entire duration of the contract. Swisscom must be notified in writing of any changes to the contact person.

8.2 Modification due to regulatory changes

In the event of new or amended regulatory or legal requirements, Swisscom may be forced to make modifications to the Enterprise App Framework or to the processes described in this service description. The Subscriber is also obliged to implement these modifications before the change takes effect. In the event of a failure to comply with this provision, Swisscom may restrict or prevent the Subscriber's use of the RA Enterprise Framework by deleting the RA Agents and depriving the Subscriber of its rights within the scope of the RA service. Any intervention of this nature on the part of Swisscom shall not constitute a breach of contract.

8.3 Identification of persons domiciled outside the EU/EEA/Switzerland

The RA Service and Swisscom Trust Services are aimed at persons domiciled in the EU, the EEA and Switzerland, as different legal provisions (e.g. consumer protection and data protection law) often apply to persons domiciled outside these regions. It is optionally possible to allow registrations for persons outside the EU, the EEA and Switzerland. This option must be explicitly ordered. The legal possibilities will then be examined and, if necessary, the terms of use or other provisions will be adapted.