Service Description
RA App Service

Swisscom Trust Services

1   Content

Swisscom Trust Services

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 for providing an RA App Service from Swisscom (hereinafter referred to as the " Service") enables subscribers to identify natural persons locally in order to sign with the signing service. The Service is provided by Swisscom (Switzerland) Ltd. and is part of Swisscom Trust Services. Identifications can be used for both advanced and qualified signatures in the EU and Switzerland.

Specifically, the employees of the subscriber can download the so-called "RA App" in the Google Play Store or Apple Store for the respective mobile device and use it for the on-site identification and registration of people physically. For this purpose, the operator of the app, the so-called "RA-Agent" is trained in advance on his identification task by means of an e-learning training before access to the app is activated. The identification uses various ID cards of the EU countries and Switzerland or passports from most countries in the world, which are machine-readable. Based on the identification process and identification data, Swisscom can offer its electronic signature service to the end-user.

For the first time, the subscriber, hereinafter "RA Agency", appoints a so-called RA-Master Agent for the provision of the service. In addition to the normal e-learning training of the RA agent, the RA-Master Agent receives a special e-learning training and access to an administration portal. This enables him to promote initially identified colleagues to RA agents or even to other RA master agents with access to the administration portal. Thus, the RA-Master Agent named by the RA Agency can ensure the complete further roll-out of the RA app in the company network.

The RA Agency is Swisscom's data processor in the field of registration. The data recorded by the RA app is cached only briefly in the volatile memory and immediately signed and encrypted by the RA agent and sent over to Swisscom. For this activity, the RA Agency concludes with Swisscom a so-called "RA-Agency Contract" in which the contractual details for the execution of the order are regulated.

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 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 Service:
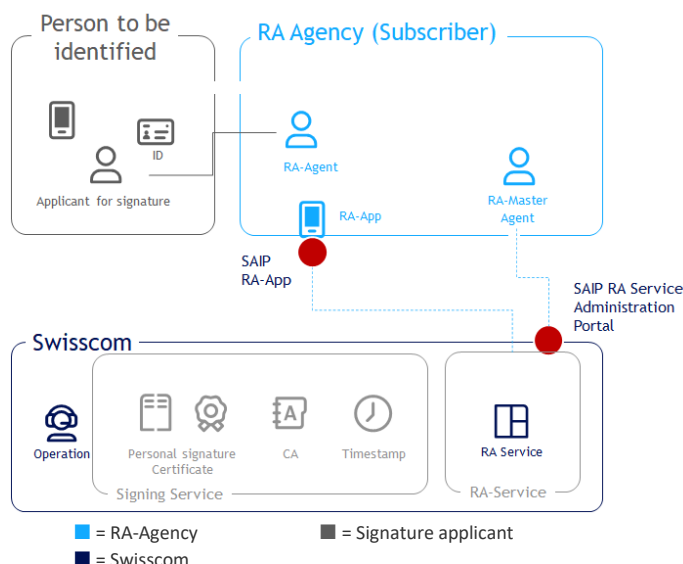
The RA Agent uses the RA-App on its mobile phone. The service access interface point (SAIP) is the the RA-App on the mobile device of the RA-Agent. In this case Swisscom is not liable for the correct installation of the RA-App on the RA-Agent's mobile phone, the correct version of the mobile operating system and the sufficient protection against attacks (e.g. virus protection). Also is Swisscom not liable on the availability of the internet or the telecommunication connections (e.g. roaming). Another service access interface point (SAIP) is the access point to the Swisscom administration portal used by - 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 RA-Agent.

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.
RA App	Swisscom development for the communication with the Swisscom backend. The app supports the taking of ID/Passport pictures and extract the necessary registration information and transfers it to Swisscom after registration.
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.
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.
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.

Term	Description
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 RA App.
RA App	Swisscom (Switzerland) Ltd. application on Android and iOS that enables identification and registration and offers the same functionalities as the RA App.
RA service	Part of the Signing Service for receiving and archiving identification data, which is operated in connection with the RA App or an RA 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. 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.
Security incident	In the RA app environment, a security incident is an event that jeopardises the confidentiality, availability or integrity of data. Examples could be: RA agents who allow incorrect identification as a favour or as a bribe. Theft of a device while an identification process has taken place. A virus on a device that has infected apps or communication or any other incident. Suspicious cases are also categorised as security incidents.
Subscriber	The subscriber is either a direct customer of Swisscom with direct service contract or has a commercial contract with a reseller of Swisscom services. In the case of RA-App the subscriber is RA-Agency. Term subscriber is also used for a party operating the signature application.
Subscriber application	The subscriber provides signatories with access to an application with which they can register for the remote signature service of Swisscom or sign. In the case of the RA app, the subscriber application scans the identity data and prepares it as evidence for Swisscom. Other subscriber applications are e.g. the signature application which is not provided by Swisscom itself.
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 App Service
RA-App available in the app store	●
e-learning	●
Administration portal	●

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

## 4.1 Definition of the service specifications and options

Specification/Option	Definition
RA-App available in the app store	The RA app is currently downloadable and installable on the mobile device from almost all stores in the EU, the EEA and Switzerland or via standard app sources. iOS and Android are supported. The access is based on a 2-factor authentication, which is activated automatically after identification for the signing service and a completed e-learning module. The RA-App is offered in the languages German and English.
e-learning	e-learning portal where a user designated by the RA Agency 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 RA App as a RA Agent. The RA Master Agent also undergoes a specially designed e-learning training.
Administration portal	Web-based application for authorised Master RA agents to manage their own RA Agent network.

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 RA Agent acts on behalf of the registration authority of the trust service of Swisscom. The RA app guides the RA agent through the identification process. This process implements the requirements that Swisscom must meet as a provider of certification and trust services.

Process description in detail:
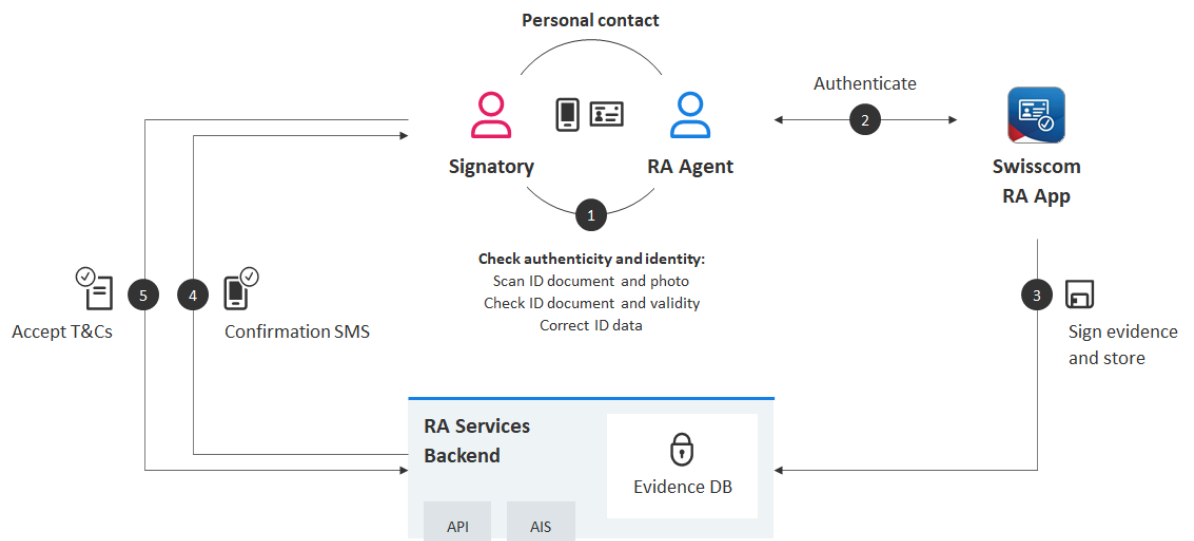
- The RA Agency shall designate a Master RA Agent within its legal entity, who can identify persons within the same entity and appoint them as RA Agents. The RA Agents can authenticate themselves using the RA App following the successful completion of the e-learning course.
- For reasons related to data 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). In addition to the mobile number, he needs the name of the registration office, which was sent to him after the agency was set up.
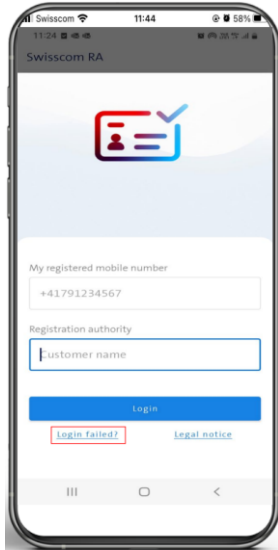
- After authentication, the RA Agent asks the person to be identified to consent to the collection and storage of his/her identification data for data protection reasons and confirms this in the app.
- The RA Agent receives the ID document.
- The RA Agent checks the photo on the ID and makes sure that it is a photo of the person to be identified.
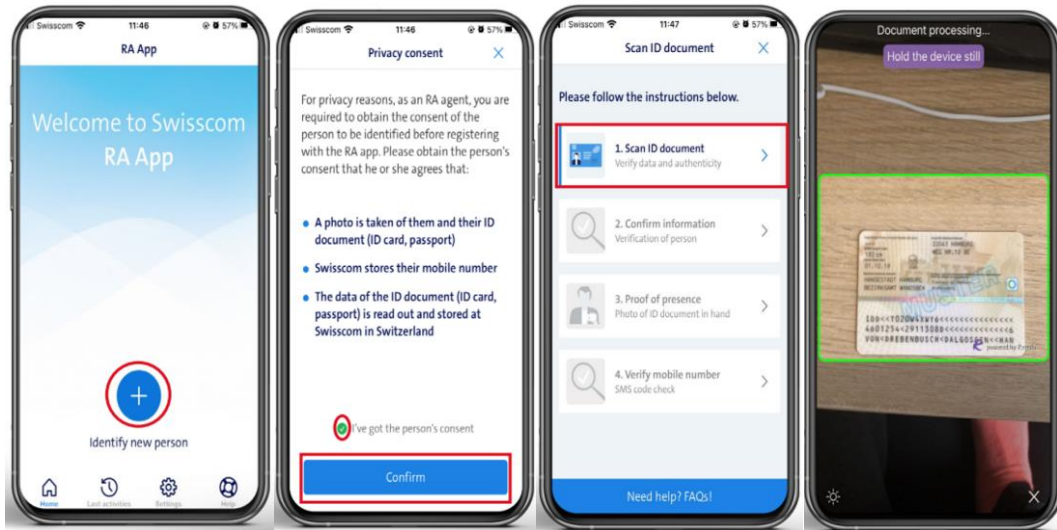
- The RA Agent takes a photo of the page of the ID document that does not contain an MRZ and then automatically triggers an app-controlled scan of the page with an MRZ. In the case of passports, only the MRZ side of the passport is scanned. The MRZ is read by an OCR.
- Afterwards, the ID is manually checked for authenticity. The app provides instructions for this by indicating the relevant haptic and visual elements based on a reference document. The data and position of this fields are provided by Regula Forensics. (see below).
- The RA agent should show the essential read contents of the ID document again to the person to be identified, so that he or she can verify the information. As a rule, the person concerned notices an OCR error in the reading of the ID document more quickly than the RA agent.
- 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 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.
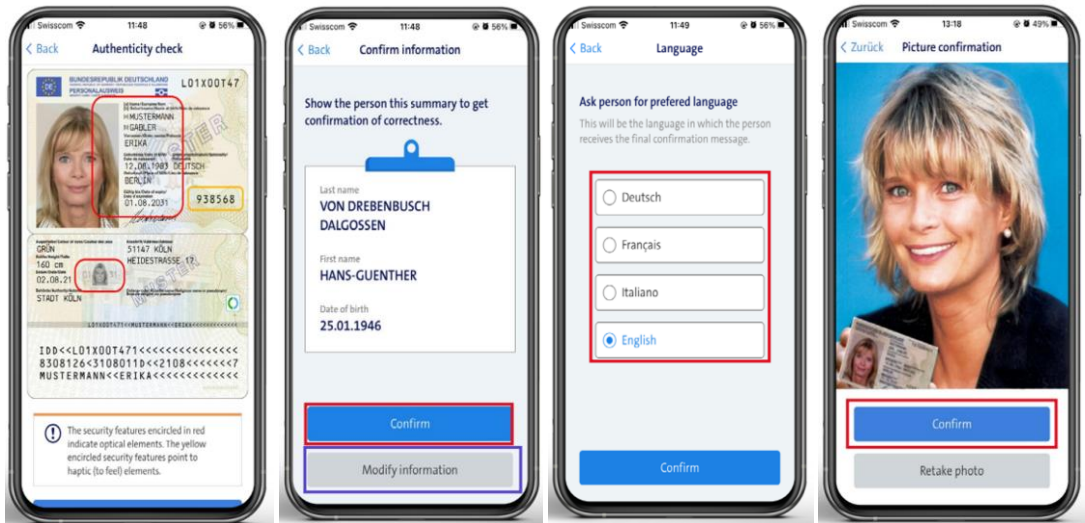
- The RA agent will then be asked to enter the mobile number of the person to be identified. The person will now receive a one-time SMS code to give to the RA agent who can enter it. The RA Agent verifies the mobile number. If the number is correct, the RA Agent can complete the registration by signing the evidence record. (3)
- The evidence signed by the RA Agent is then transmitted to Swisscom's Signing Service as evidence.
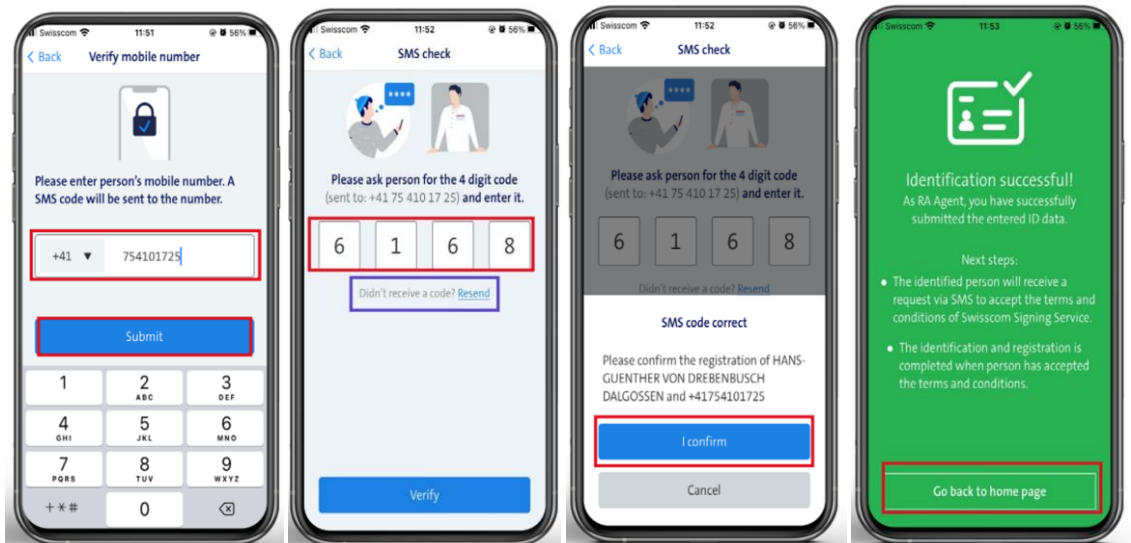
- After this, Swisscom sends an SMS containing a URL to the terms and conditions of use to the identified person.
- To use the Swisscom certification service, the identified person still has to confirm the terms and conditions of use by clicking on the link in an SMS sent to them and confirming the terms 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 person has rejected the terms and conditions of use or at the latest after 15 days without a reply from the user.

4.2.2   Use of Regula Forensics

Regula Forensics is a company busy for 30 years in the automatic border control area and has a strong cooperation with Interpol, Europol and national banks. They have a comprehensive database indlcuding over 12000 identity document templates from 248 countries and territories. As soon as the type of ID document is analyzed Regula Forensics is contacted via SDK in order to supply the correct template and the zones for security features in order to support the RA-Agent's manual process of fraud detection of the RA-Agent in the RA-App.

4.2.3 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 RAagents 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 user (archive the data set)

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 RA Master Agent at the time of setup.

4.2.4 Data to be transmitted

The following data will be transmitted as evidence to Swisscom:

- Mobile number
- Surname
- First name of the identified person
- 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 RA 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.

4.2.5 Supported countries

All supported ID cards and passports are continuously updated on a document to be found at
https://trustservices.swisscom.com/downloads "Country list RA App".

4.2.6 Signature approval methods

The RA-App supports the following signature approval methods:

- Mobile ID
- Mobile ID App
- Password / One time code via SMS

for subsequent signatures. The approval methods are described in the "Service Description Registration and Signature Approval Methods".

4.2.7 Onboarding process

The RA Agency nominates a RA-Master Agent in the contract. The RA Master Agent must first register for the signing service itself. This is possible in the Swisscom Shop of Switzerland, via any RA agent (e.g. employees of a partner of Swisscom or Swisscom) or via a video identification. In the case of a video identification, 2 vouchers will be provided to the RA Agency for this purpose.

The RA Agent follows a e-learning program independently and fulfils the necessary tests. With the setup of a new RA agency Swisscom will send out an email and invite the RA-Master Agent to participate to a special RA-Master Agent e-learning training. The RA Master Agent then gains access to the RA app and the administration portal and can start the identification and also the roll-out of the app in the company.

4.3 Service description for the RA Agent network and training process

After the first Master RA Agent is appointed has fulfilled the e-learning test 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 employees of the RA Agency 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 RA Agency to independently create an entire network of Master RA Agents and RA Agents:
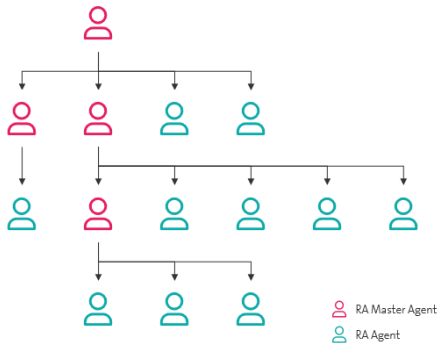
As soon as an RA Agent or Master RA Agent is appointed, that RA Agent or Master RA Agent receives an invitation to undergo RA Agent training. This request is sent via SMS and contains a link to Swisscom's e-learning platform, which the RA Agent or Master RA Agent can use to independently start taking 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 RA 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 RA App in order to ensure that RA Agents have the knowledge they need to perform identifications. In accordance with the RA Agency contract, the RA Agency 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 Agency contract with the RA Agency for the RA App.

5   Service provision and responsibilities

Non-recurring services

Activities (S = STS/RA = RA Agency)	S	RA
Provision of service		

Swisscom Trust Services

Activities (S = STS/RA = RA Agency)	S	RA
1. Provision of the service infrastructure, general RA service for the operation of the RA App: This includes the administrative portal for managing the identified persons, RA Agents, the RA service backend, as well as the e-learning module.	✓	
2. Sending the signed RA Agency contract for the RA App in connection with the use of the RA App and the appointment of the first Master RA Agent		✓
3. Setting up the e-learning trainings of all (Master) RA Agents	✓	
4. Activation of the RA Agency in the RA service and entry of the Master RA Agent as designated in the RA Agency contract	✓	
5. Provision of an administrative portal for the designated Master RA Agent to appoint additional RA Agents and Master RA Agents	✓	
6. Provision of access to an e-learning course for identification tasks in the RA App	✓	
7. Controls access to RA App functions depending on a user's e-learning status	✓	
8. Service maintenance and release management	✓	
Termination of the service		
1. Notification of the relinquishment of business activities, a bankruptcy notice against the RA Agency, the opening of bankruptcy proceedings or a debt restructuring moratorium		✓
2. Deletion of authorisations and access for all of the RA Agents and Master RA Agents	✓	
3. Deletion of the administrative area for the RA Agency that was created for the RA Agency	✓	

Recurring services

Activities (**S = STS/RA = RA Agency**)	S	RA
Standard services		
1. Operation of the Service incl. interfaces, administrative portal and e-learning infrastructure	✓	
2. Lifecycle management of the RA App (interface modifications, integration of new versions of the RA App Framework, security patches, additional security assessments)		✓
3. Lifecycle management of the infrastructure : Updating to the current status of technology and security (security patches, updates etc.) for the protection of identification data		✓
4. Amendment of the definition of the security requirements	✓	
5. Ensuring the use of technical means of authentication and contractually agreed authentication methods (e.g. Mobile ID, PWD/OTP)		✓
6. Provision of support services (service desk, incident management, etc.)	✓	
7. Reporting of changes to -specific information of the RA Agency(contact persons, name of the organisation, etc.)		✓
7. First training of the Master RA Agents appointed by the RA Agency to use the administrative tool and Signing Service their awareness of regulatory requirements	✓	
9. Careful selection and management of RA Agents (only RA Agents within the organisation, delete agents when they leave the organisation, etc.)		✓
10. RA Agent training by means of the e-learning process provided by Swisscom		✓
11. Reporting security incidents that affect the RA service to the following e-mail address: all-in.signingservice@swisscom.com		✓
12 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 availa-ble for each variant, the service level is selected in the service contract..

Service levels & target values			RA App Service	
			RA service Admin portal	RA App
Operation time				
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	Best effort		●	●
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.

---

[1] If the 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.

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 RA App Service 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 RA Agency and the 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.

8 Special provisions

8.1 Data processing by Swisscom

The data collected by the RA App will be processed for Swisscom IT Services Finance S.E. as eIDAS trust service and for Swisscom (Schweiz) AG as ZertES certification service in Switzerland. RA-Agents can operate worldwide as long as they follow the data processing regulations of EU and Switzerland concerning third party countries.

8.2 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.