Service Description

All-in Signing Service for personal signatures in the EU

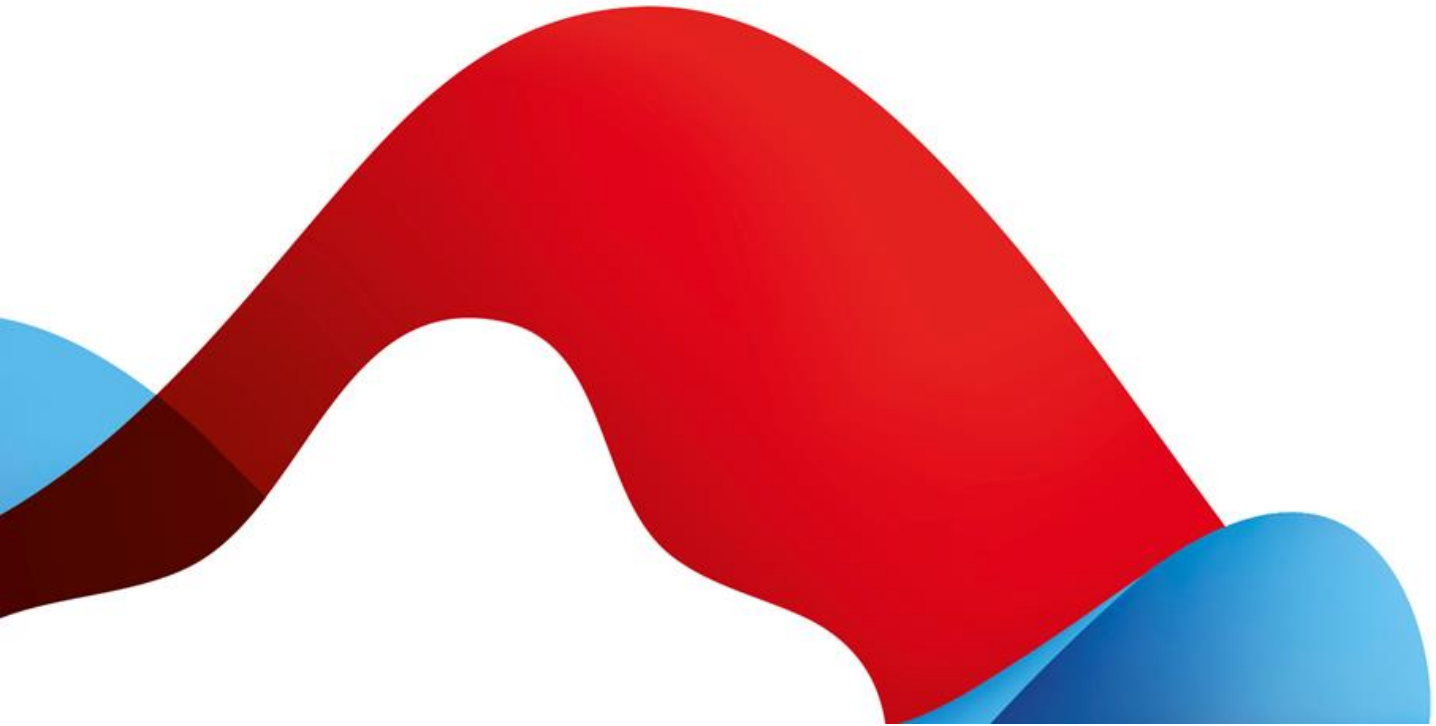
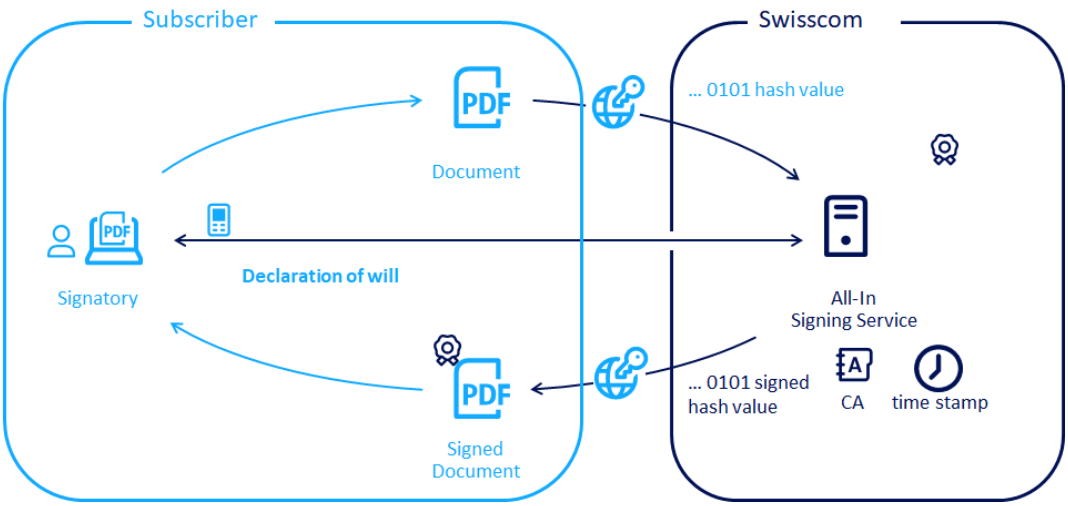


Table of contents

1 Service overview

The All-in Signing Service (AIS) in accordance with this service description is a server-based remote signature service provided by Swisscom IT Services Finance S. E. , Vienna (AT), hereinafter referred to as "Swisscom ITSF". The AIS is provided in the data centres of Swisscom (Switzerland) Ltd. in Switzerland and Swisscom (Switzerland) Ltd. distributes the AIS in its own name or grants third parties the right to distribute the AIS in its own name. It enables signatories to electronically sign digital files and thus ensure the integrity and authenticity of a file. The qualified trust service of Swisscom ITSF creates and manages the signature certificate for the signatories as a fiduciary and makes it available to the remote signature service via an encrypted channel. Apart from a subscriber application for the sending and receipt of the signed document, the signatory does not require any other operating equipment, such as tokens or signature cards.

The subscriber application prepares a document so that for signing only the hash value (check sum of fixed length without any indication of the content) has to be sent to AIS. The effectively readable files and the information they contain do not leave the Subscriber's system environment and cannot therefore be viewed by Swisscom. The signed hash is reintegrated into the document by the subscriber application and thus creates a signed document. Before activating the signature, the Subscriber has to be authenticated by the subscriber application and declare their consent to sign. The All-In Signing Service uses various possible authentication methods.



The signatories can identify themselves beforehand using a procedure approved according to eIDAS (e.g. "RA-App", own registry) and then use an associated authentication for each signature.

With regard to the signatures, a general distinction is made between advanced and qualified electronic signatures. Qualified electronic signatures have the highest degree of legal validity and have the same status as a handwritten signature in many cases. This means that in many cases the handwritten signature can be replaced (see section 7.2).

Swisscom ITSF is a recognised provider of signature and certification services in Austria for the issuance of qualified certificates for electronic signatures and electronic seals in accordance with the eIDAS Regulation and the Austrian Signature and Trust Services Act (SVG). A conformity assessment body regularly checks whether the requirements made of providers of certification services by European and Austrian law and/or recognised technical norms are also met. The supervisory authority grants Swisscom ITSF qualification status as a qualified trusted service provider. Swisscom ITSF is included on the trust lists in accordance with Art. 22 of the eIDAS Regulation and is entitled to use the EU trust mark.

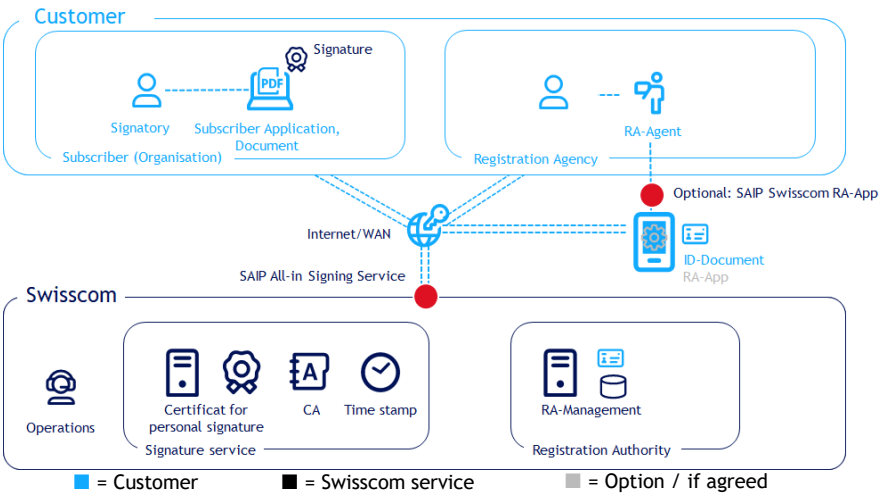
Swisscom's AIS Service generally provides advanced electronic signatures for natural and legal persons and qualified electronic signatures for natural persons depending on the contract structure and selection of the Subscriber. This service description describes the service for electronic signatures for natural persons in the EU and EEA states that have implemented the eIDAS regulation.

2 Definitions

2.1 The 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 schematic diagram illustrates the services and service components of the All-in Signing Service:



The service provision point for the signatures is Swisscom's connection to the Internet. SMS information is provided at the interface to the roaming partner, unless it is provided within the Swisscom network. A service promise for the proper performance of the Internet or the network operation of the roaming partner is excluded.

2.2 Service-specific definitions

Term	Description
AIS service	All-In Signing Service
CMS	Cryptographic Message Syntax – a syntax defined in RFC5652 for the digital signature and cryptographic messages.
CP/CPS	Certificate guidelines (CP/CPS) for issuing certificates of the “Diamond” (qualified) and “Sapphire” (advanced) classes. Certification guidelines, certification practice, documents of a certification authority which describe the guidelines and practice for issuing certificates.
Distinguished name	Standardised form to describe a certificate subject. The subject of a certificate clearly designates the identification of the signatory.
Document	For the sake of clarity, the term document is used synonymously with the term data. Both documents and data can be signed.
eIDAS regulation	Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC). This Regulation shall in particular also regulate the electronic signature.
Electronic signature	The electronic signature is a technical procedure for checking the integrity of a document, an electronic message or other electronic data and the identity of the signatory.
Hash	Clear depiction of a large amount of data on a small amount of data, almost like a document’s fingerprint. The document contents cannot be traced from the hash.

Term	Description
Mobile ID	Managed Service for secure user authentication. Mobile ID can be used in Switzerland in combination with a mobile subscription of any Swiss mobile provider, e.g. Swisscom.
Mobile ID App	Managed Service App downloadable from the Google Play Store or Apple store for secure user authentication based on offered authentication means of the mobile device like fingerprint, face recognition, etc. Initialization is done by use of the mobile number. The Mobile ID App can be used with any international mobile number and by use of an Internet connection.
OASIS DSS	Interface standard for digital signatures for web services and other services of the OASIS Group (non-profit organisation for open standards in IT)
On-demand signature	Term frequently used in technical documents for the “personal signature” in accordance with this service description.
OTP	One Time Password – Password created for use on one occasion which is sent via SMS.
PKCS#1	Cryptographic standard of the RSA Laboratories.
PWD	Password (entry) for the authentication of the password to be used for the service.
RA agent	Authorised operator of the RA app.
RA agency	Organization providing the RA agents.
RA app	App (application) which can be downloaded from the Android or iOS store. This enables a trained RA agent to carry out identification for advanced and qualified signatures and sends the data to the RA service.
RA service	Service for receiving and archiving the identification data, operation in relation to the RA app.
Registration authority (RA)	Authority responsible for the identification of the signatories. May be provided by the Subscriber, Swisscom or third parties provided a contractual relationship with Swisscom exists.
REST	Representational State Transfer, programming paradigm for distributed systems, particularly web services.
Secure signature creation unit (HSM)	Qualified and certified hardware for creating signature keys and signature certificates.
Signing	Natural person who signs a document electronically after prior identification, authentication and declaration of consent.
SOAP	Simple Object Access Protocol – alternative interfaces, programming paradigm concerning REST for web services.
SSL/TLS	Secure socket layer, transport layer security, encryption protocol for secure data transmission on the internet based on SSL (access) certificates.
Smart Registration Service	Additional service of Swisscom with online identification methods which import the evidence data also into the RA-Service in the same way as the RA-App
Subscriber	Swisscom provides the services in accordance with this service description for the benefit of the Subscriber. The Subscriber is either a direct client of Swisscom with an All-in Signing Service contract (including the existing configuration and acceptance statement) or has a commercial contract with a partner of Swisscom with a configuration and acceptance statement vis-à-vis Swisscom. This acceptance and configuration statement is valid as a “Subscriber Agreement” in accordance with the ETSI norm EN 319 411 for fiduciary service providers.
Subscriber application	The Subscriber provides the signatories with access to an application with which it can create electronic signatures in accordance with the terms and conditions of use and the Subscriber ensures the transmission of signature data to the remote signature service of Swisscom as well as the authentication (“subscriber application”). The subscriber application

Term	Description
	receives the signed data and prepares the document for the signatories. The signature service provides an interface linked to a subscriber application to activate the signature. The subscriber application is not part of this service description. It is provided outside of the All-In Signing Service, for example by partners.
Terms and conditions of use	The terms and conditions of use govern the terms for using the signature certificates and signature service in the relationship between Swisscom IT Services Finance S.E. and the signatory on a subscriber application. They can be viewed at https://www.swisscom.ch/en/business/enterprise/offer/security/digital_certificate_service.html

3 Variants and options

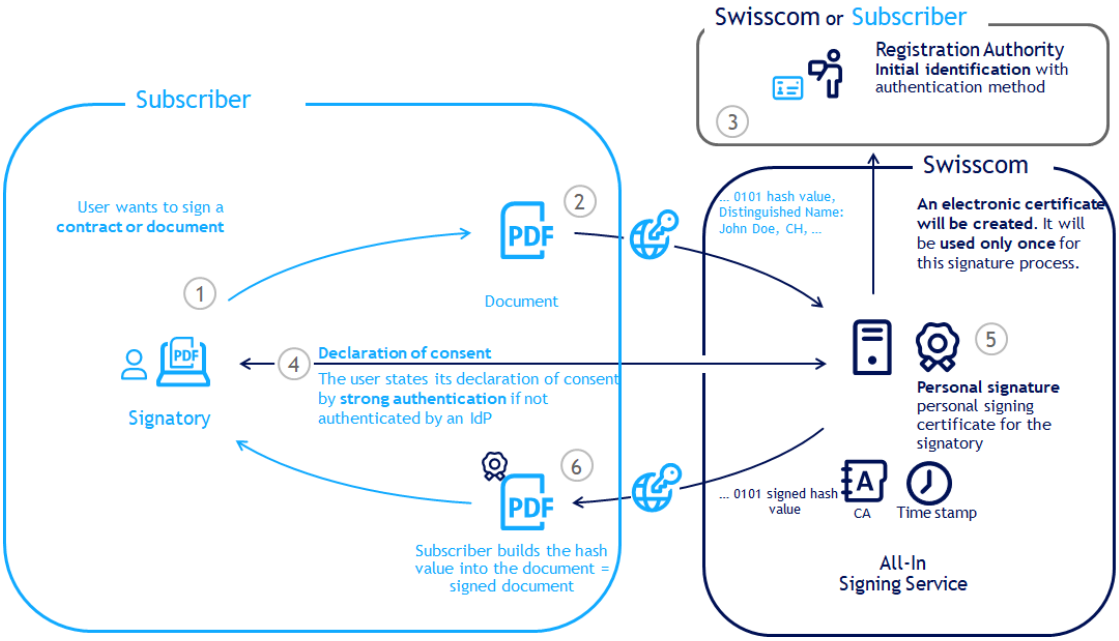
Standard variant	Electronic personal signatures
Qualified electronic signature	●
Advanced electronic signature	●
Electronic time stamp	●
Identification with RA app	●
Other identification procedures	○
Other procedures for declaration of consent that differ from the standard (PWD/OTP or Mobile ID App)	○
Operation in accordance with certification guidelines (CP/CPS)	●

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

3.1 Definition of the services

Service	Definition
Qualified electronic signature	Qualified electronic signature in accordance with Art. 3 No. 12 eIDAS-VO.
Advanced electronic signature	Advanced electronic signature in accordance with Art. 3 No. 11 eIDAS-VO.
Electronic time stamp	Electronic time stamp within the meaning of Art. 3 No. 33 eIDAS Regulation which does not meet the requirements of the qualified time stamp according to Art. 3 No. 34 eIDAS Regulation.
Identification with RA App	The customer can sign a RA-Agency contract free of charge in order to use the RA-App for a face-to-face identification
Other identification procedures	Optionally other identification procedures can be used by signing additional service contracts (e.g. Video Identification) or a customer specific identification procedure can be authorized for use
Other procedures for declaration of consent that differ from the standard	Optionally the customer can request the authorization to use other procedures for the declaration of will. It requires always an audit.
Operation in accordance with certification guidelines (CP/CPS)	The operation of a certification service provider is based on the EU certificate guidelines (CP/CPS) for issuing certificates of the “Diamond” (qualified) and “Sapphire” (advanced) classes. The latest version can be viewed here: https://www.swisscom.ch/en/business/enterprise/offer/security/digital_certificate_service.html

3.1.1 Signature creation procedure for all options



- The subscriber application is linked to the Swisscom AIS service using a SSL/TLS access certificate.
- The signatory logs into their subscriber application (1) and selects the document to be signed. The subscriber application creates a hash in accordance with Swisscom provisions (2) and sends it to the AIS service. Information relevant to the signature certificate subject is also sent by the subscriber application. If the Subscriber is recorded by the registration authority and authorised for the signature, the AIS requests the declaration of consent from the signatory. (4)
- If the registration authority of Swisscom is used with the RA app or the Smart Registration Service, the signer must be identified before placing the first signature and associated with a method of expressing will (authentication method). The transferred signature data of the subscriber application will be compared with the identification data of the Swisscom registration authority. (3)
- Qualified signature certificates and signatures are only created on the basis of 2-factor authentication which is carried out e.g. by PWD/OTP, Mobile ID App or another certified authentication method.
- The key material (private and public keys) as well as signature certificates, which are necessary for the advanced or qualified electronic signature (incl. time stamp), are created. (5) The key material is generated and used - under the responsibility of Swisscom ITSF - on the AIS service at Swisscom (Switzerland) Ltd. An advanced or qualified signature certificate is issued for this key pair in accordance with the certification guidelines of Swisscom ITSF and the subject of the signature certificate sent by the subscriber application (distinguished name). The signature certificate and the key pair are used for a single signature request by the Subscriber and the key pair is deleted after use. Personal signature certificates are generally valid for a few minutes.
- Signing of the hash value (cryptographic check sum of a data set/text of any length) to safeguard its integrity according to the CMS or PKCS#1 standard.
- Return of the signature as well as any additional validation information in the signature certificate (e.g. certificate chain for the trustworthy root certificate and qualified time stamp). The subscriber application ensures the signature of the document based on the signed hash. (6)

3.2 Processes and tools for personal identification (registration authority)

Before expression of wil can be carried out, the signatory must identify themselves in accordance with the requirements of the type of electronic signature concerned. The identification process can be carried out separately from the signature process at a registration authority and Swisscom provides several variants.

3.2.1 Overview

Identification process	Suitable for qualified signature eIDAS	Suitable for advanced signature eIDAS	
Standard procedure for RA app in accordance with 3.2.2	✓	✓	
Standard procedure with Smart Registration Service in accordance with 3.2.3	(✓)	(✓)	Depending on the identification method of the Smart Registration Service
Own registration authority with different identification procedure in accordance with 3.2.4	(✓)	(✓)	Depending on the separate agreement in the implementation concept and in the contract for the delegation of personal identification

3.2.2 RA app standard procedure with separate contract

Swisscom provides an RA app from Swisscom (Switzerland) Ltd. for carrying out the personal identification of the signatory. Swisscom (Schweiz) Ltd. has been designated by Swisscom ITSF as the registration authority. It is operated by the RA agent who generally belongs to the Subscriber's organisation or to a third organisation proposed by the Subscriber or Swisscom. The organisation providing the RA agents is called the "RA Agency" and concludes a separate RA Agency Contract. The RA Agency commits by contract to Swisscom to carry out the personal identification on behalf of and in the name of Swisscom using the app made available in accordance with the process specifications of Swisscom and to send it to the registration authority at Swisscom. Each RA agent will receive a list of its duties of confidentiality and cooperation after successful training. The registration authority therefore remains at Swisscom with the RA app which runs on Android and iOS. Swisscom may withdraw the status as an RA agent from an RA agent and thus this person's entitlement to operate the RA app without notice and at any time and without providing justification.

The RA app requests the RA agent to firstly select the issuing state and the nature (ID, passport) of the identification document. The zones for the haptic and visual check are then shown on a model of the selected document with which the authenticity of the document can be checked. The front and back of the document are then photographed. n OCR automatically determines the identification data required from the machine-readable zone of the document. They must be checked for read errors and corrected. A photo of potential signatory with a background of the environment where the check is carried out (e.g. table, characteristic wall paintings) provides evidence of the physical presence during the check. The potential signatory then receives a call on a previously entered mobile telephone number to confirm the correctness and ownership of the mobile phone number. Once the identification has been completed, the signatory must confirm and sign the terms and conditions of use of the Swisscom ITSF AIS service and they click on the link in a SMS sent from the AIS Service and confirm the terms and conditions indicated therein.

A person who has been identified by the RA app thus becomes a "community member" of the Swisscom ITSF signatories and can have a valid personal signature created for the duration of the period of validity of the identification with all AIS subscribers of Swisscom ITSF and optional of Swisscom (Switzerland) Ltd. without new identification being required provided this is permitted by the subscriber application concerned.

Swisscom may designate RA master agents based on applications of the RA Agency who can propose further RA agents independently within the same organisation so that an entire network of RA agents can be established within an organisation. The RA master agents are subject to separate Swisscom terms and conditions.

3.2.3 Smart Registration Service standard procedures

Swisscom provides further standard online identification procedures within an additional service called "Smart Registration Service". An example is the video identification. Please refer to the service description of this service concerning more details of the different procedures. All identifications are done in combination with the registration of the mobile phone number which is used during the signing process as authentication means.

The methods offered by Swisscom of the Smart Registration Service are subject to a separate additional contract for this service and are not part of this service description (see Service Description Smart Registration Service).

3.2.4 Project-specific registration authority

If the Subscriber does not wish to use the aforementioned procedure for the identification of signatories and wishes to set up its own registration authority with project-specific identification or to otherwise differ from the aforementioned standard procedures, this will be agreed beforehand with Swisscom. The Subscriber must conclude a delegation agreement for identification of personal signatures (RA delegation agreement) with Swisscom (Switzerland) Ltd. and present an implementation concept prior to the contract comes into force which is checked and evaluated by Swisscom. As a rule, the conformity assessment body and the supervisory body must also approve these project-specific registration authority processes for the issue of qualified signature certificates.

3.2.5 Organisation check process

If the organisation associated with the potential signatory is also determined in the aforementioned procedure on personal identification, an organisation check is also carried out in accordance with the provisions of CP/CPS before commencement of the service by Swisscom ITSF. This must also be indicated in the acceptance and configuration statement and an authorised representative of the organisation must have signed the acceptance statement. By signing he/she also grants consent for the use of the organisation name in relation to the signatories.

3.3 Data storage and responsibilities

3.3.1 Standard procedure in accordance with paragraph 3.2

With the use of the Swisscom RA app or the Smart Registration Service, the data on the identified person and the identification documents and evidence of acceptance of the terms and conditions of use are only stored on servers of the Swisscom registration authority in Switzerland and are retained for the periods in accordance with CP/CPS or under law.

3.3.2 Project-specific procedure in accordance with paragraph 3.2.4

For project-specific procedures, the storage and place of storage are set out in the separate agreement on the delegation of personal identification with implementation concept.

3.4 Declaration of consent

Every personal signature requires the submission of a declaration of consent or will by the signatory. The authentication method used during the identification of the signatory is used for the declaration of consent or an expression of consent has already been made during the identification.

Various procedures are available for the submission of the declaration of consent itself:

- PWD/OTP: Here signatories authenticate themselves to the AIS service via a password entry page, which they receive via SMS, in the AIS service and activate the generation of a one-time password on the service which is sent via SMS to the mobile phone of the signatory. The signatory enters this in the subscriber application.
- OTP: The authentication of the signatory in the AIS Service is omitted in this procedure and instead the signatory sends a one-time password directly to the AIS service which is sent to them beforehand via SMS. This procedure can only be used for advanced signatures.
- Mobile ID: Currently only usable with MobileID-enabled SIM cards from Swiss mobile phone providers. This enables the signer to authenticate himself for a signature using direct 2-factor authentication and to trigger an expression of consent for the signature. If Mobile ID is not available for the mobile phone number, the PWD/OTP procedure is automatically used. This variant can be carried out on simple mobile devices (i.e. no smartphone required). Mobile ID: Currently only usable with MobileID-enabled SIM cards from Swiss mobile phone providers. This enables the signer to authenticate himself for a signature using direct 2-factor authentication and to trigger an expression of intent for the signature. If Mobile ID is not available for the mobile phone number, the PWD/OTP or Mobile ID App procedure is automatically used. This variant can be carried out on simple mobile devices (i.e. no smartphone required).
- Mobile ID App: This Authenticator app can be used as long as the standard Mobile ID procedure is not in use. It is also suitable for international mobile use outside Switzerland. The signer triggers a 2-factor authentication by means of a biometric feature enabled by the device or a PIN/password. For this

purpose, the app must be installed before the first use, e.g. before the confirmation of the terms of use, and initialized with the mobile number. A smartphone connected to the Internet is required.

- Project-specific declaration of consent: If the aforementioned procedure is not used, any project-specific declaration of consent procedure will be agreed beforehand with Swisscom. The Subscriber must present an implementation concept prior to the conclusion of the contract which is checked and evaluated by Swisscom. Individualised declaration of consent processes must generally also be approved by the certification authority or conformity assessment authority for certification services for subscribers.

4 Performance description and responsibilities

4.1 Signature service

Non-recurring services

Activities (S = Swisscom/SB = Subscriber)		S	SB
Provision of the service			
1.	Provision of the AIS infrastructure	✓	
2.	Provision of the SAIP interface based on the OASIS DSS protocol via SOAP or REST. Alternatively, interface via OAuth2.0 according to standard ETSI TS 119 432. The interface can be found at http://documents.swisscom.com/product/1000255-Digital_Signing_Service/Documents/Reference_Guide/Reference_Guide-All-in-Signing-Service-en.pdf	✓	
3.	Sending of signed acceptance and configuration statement with activation-relevant information and the required designation of roles (system administrator, security officer).		✓
4.	Organisation entry in the signature certificate option: Provision of all necessary documents for the organisation check at the request of Swisscom (e.g. attested commercial register extract). Signature in the acceptance statement by an authorised representative of the organisation for the consent that the organisation agrees with the entry of the organisation's name in the signature certificate for the signatories.		✓
5.	Organisation entry in the signature certificate option: Check of the authorisation to enter the organisation's name in the signature certificate.	✓	
6.	Sending of a publicly trustworthy or self-signed SSL/TLS authentication certification for the authentication vis-à-vis the AIS server and for encrypted communication with the AIS service. For specifications see acceptance statement.		✓
7.	Activation of the communication to the subscriber and option IdP for the access certificate sent.	✓	
8.	If required, configuration of the firewall, on the server side at the Subscriber's site.		✓
9.	Designation of a person responsible including constant deputation for all matters concerning technology, security and the implementation of registration of signatories and contact partners for audit matters.		✓
10.	Connection of the Subscriber and sending of subscriber-specific access data.	✓	
11.	Integration of the AIS service into subscriber-specific application(s) and/or subscriber side connection of the interface to AIS, e.g. through the use of a partner application.		✓
12.	Checking of the connection to the AIS server and/or the issuing of signatures. Immediate notification of any errors before the signatures are used.		✓
13.	Fault rectification through update or re-installation.	✓	
14.	Notification of the relinquishment of business activities and any bankruptcy notices against it, the opening of bankruptcy proceedings or a debt restructuring moratorium.		✓
Termination of the service			
1.	Deletion of subscriber authorisations in the AIS infrastructure.	✓	
2.	Deletion of the key from the HSM.	✓	

Recurring services

Activities (S = Swisscom/SB = Subscriber)		S	SB
Standard services			
1.	Operation of the AIS infrastructure.	✓	
2.	LifeCycle management of the AIS service infrastructure.	✓	
3.	LifeCycle management of the infrastructure of the systems connected to the All-in Signing Service: Modification of the current status of technology and security (security patches, updates etc.)		✓
4.	Appropriate technical and organisational measures to protect the data (e.g. including through the deactivation of connections not required or access regulations etc.). Disclosure of the security system of the application and communication to Swisscom if requested by Swisscom ITSF or its conformity assessment body or supervisory body.	✓	✓
5.	Modification of the definition of the security requirements.	✓	
6.	Lifecycle management of its access certificate, timely exchange upon expiry of validity by the designated security manager by e-mail to servicedesk.ict@swisscom.com with designation of the account name. Avoidance of any disruption of the SSL/TLS connection (e.g. through “inspection” module).		✓
7.	Creation of signature certificates based on the X.509 standard.	✓	
8.	Definition of the signature certificate content and procedure for signature creation.	✓	
9.	Ensuring the use of technical means of authentication and contractually agreed authentication methods (e.g. PWD/OTP, Mobile ID App).		✓
10.	Sending of the signatory’s data (distinguished name) in accordance with the provisions of the acceptance and configuration statement.		✓
11.	Implementation of signatures for which the signatory’s declaration of consent exists.	✓	
12.	Signature is provided in conjunction with a time stamp.	✓	
13.	Meeting the cooperation obligations and requirements by the security officer.		✓
14.	Provision of support services (service desk, incident management, etc.)	✓	
15.	Reporting of changes to subscriber-specific information (contact persons, access certificate, etc.)		✓
16.	Updating of subscriber-specific information (contact persons, access certificate, etc.)	✓	
17.	Reporting of security incidents on the system of the subscriber application or IdP system which concerns the AIS service.		✓
18.	Reporting of security incidents on the system of the signature service which has an impact on subscribers.	✓	
19.	Decision-making and responsibility for the legal implications of the signature type selected (see section 7.2)		✓
20.	Notice to signatories in the user interface of the subscriber application or in the question regarding expressions of intent about the type of signature used.		✓
21.	Modification of the interface in line with Swisscom’s new requirements within 3 months due to regulatory or security requirements.		✓

4.2 RA app for personal identification

Non-recurring services

Activities (S = Swisscom/SB = Subscriber)	S	SB
Standard services in case of optional use of the RA-App		
1. Conclusion of a RA Agency Contract with the RA Agency for the purpose of enabling the personal identification of RA Agents using the Swisscom RA App as described in Section 3.2.2 of this Service Description.	✓	
2. Consultation with the RA Agency proposed by the Subscriber to ensure that any termination of the RA Agency Contract by the RA Agency complies with the Subscriber's requirements.		✓
3. Cooperation for the development and integration of a new identification process in accordance with the possibilities of this service description (cf. Subclause 3.2.1) in the event of termination of the RA Agency Contract.	✓	✓

Recurring services

Activities (S = Swisscom/SB = Subscriber)	S	SB
Standard services in case of optional use of the RA-App		
1. Identification of signatories, registration of additional RA (Master) agents in accordance with RA agency contract		✓
2. Activation of the signers for the signature, operation of a portal for the administration and registration of all RA agents, further master RA agents and signed persons.	✓	

4.3 Own registration authority, video identification

Non-recurring services

Activities (S = Swisscom/SB = Subscriber)	S	SB
Standard services in case of optional use of the RA-App		
1. Conclusion of a contract for the delegation of personal identification ("RA delegation contract") in order to enable the personal identification to be carried out by an own registry according to an implementation concept and/or certification	✓	
2. Preparation of an implementation concept for the operation of the registration authority with relevant information (registration process, consent to the declaration of use, archiving of registration data, data transfer after termination of business activity, registry officer and organisation, system and network security concept, data protection) and/or presenting a corresponding certification according to ETSI (advanced) or eIDAS (qualified)		✓
3. Cooperation in the development and integration of a new identification process in accordance with the possibilities of this description of services (cf. subsection 3.2.1) in the event of termination of the RA delegation agreement.	✓	✓

Recurring services

Activities (S = Swisscom/SB = Subscriber)	S	SB
Standard services in case of optional use of the RA-App		
1. Identification of signatories		✓
2. Activation of the signers for the digital signature	✓	

5 Service levels and reporting

5.1 Service levels

The following service levels generally relate to the agreed support times. Definitions of terms (Operation Time, Support Time, Availability, Security and Continuity) and the description of the measurement method and reporting are set out in the other contract elements (e.g. SLA Definitions).

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 level & target values			Electronic personal signatures
Operation Time			
Operation Time	Mo-Su 00:00-24:00		
Provider Maintenance Window	PMW-DC	PMW Data Center Swisscom	●
	PMW-S With advance notice for security and system-critical updates	Daily 19:00-07:00, only for announced maintenance	●
Support Time			
Support Time	Mo-Su 00:00-24:00		●
Fault acceptance	Mo-Su 00:00-24:00		●
Availability			
Service Availability			
▪ Signature service	99.8%		●
▪ Directory services according to CP/CPS section 3.1	99.9%		●
Security			
	Advanced (ITSLA)		●
	Customised (ITSLC)		○
Continuity			
ICT Service Continuity (ICTSC)	RTO 120 h | RPO 24 h		●
	RTO 48 h | RPO 24 h		○

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

5.1.1 Support and Operation

During the support time, Swisscom ensures the operation of the AIS service in accordance with SLA clause 5.1 up to SAIP. Faults can be reported and accepted during this time (1st Level Support). If the AIS service has been purchased through a Swisscom partner, it must be contacted in the event of malfunctions. The partner will forward the fault to Swisscom if he cannot remedy it. Customer specific issues and service setups are handled by the 2nd Level Support Monday to Friday from 8h00 to 17h00. The holiday regulations of the basic document "SLA definitions" must be considered.

5.2 Service level reporting

Within the scope of the service, the Subscriber receives the following standard service level report. Further reports can be provided, subject to charge, as part of the advanced reporting service after assessing the feasibility of the Subscriber's requirements.

Service level report		Electronic personal signatures	Reporting period
Availability	Service availability of the service		
	▪ Signature service	● (on request)	Month
	▪ Directory services	● (on request)	Month

● = Standard (included in price)

6 Billing and quantity report

6.1 Billing

Services are billed retroactively for the previous month. The billing details are governed by the service contract.

6.2 Quantity report

Quantity reports are governed in the service contract.

7 Special provisions

7.1 Subscriber application

The subscriber application is not part of this service description. It is provided by the Customer itself, by a Swisscom partner or by Swisscom ITSF or Swisscom (Switzerland) Ltd. itself.

7.2 Signature types and their applications

It is the Subscriber's responsibility to obtain professional clarification of the legal implications of the selected type of electronic signature (with and without time stamp) made available to the signatories. Swisscom accepts no responsibility in this regard.

Qualified electronic signature (QES, Swisscom diamond class certificate): The QES created via the AIS meets the characteristics defined in the CP/CPS and the definition in accordance with Art. 3 eIDAS-VO with the legal effects referred to in Art. 25 eIDAS-VO.

Electronic time stamp: The electronic time stamp created using the AIS meets the characteristics defined in the CP/CPS and the definition in accordance with Art. 33 No. 33 eIDAS Regulation. It is not a qualified electronic time stamp according to Art. 3 No. 34 eIDAS-VO.

Advanced electronic signature (AES, certificate of Swisscom sapphire class): The AES created via the AIS meets the characteristics defined in the CP/CPS and the definition according to Art. 3 eIDAS-VO with the legal effects referred to in Art. 25 eIDAS-VO. The AES does not have the same legal validity as a handwritten signature.

Depending on the situation, some documents therefore require the handwritten signature or the QES with a electronic time stamp in order for the intended legal validity to enter into effect at all.

The validity of electronic signatures created via AIS in accordance with the certificate guidelines (CP/CPS) for the issuing of signature certificates issued by the issuing CAs "Diamond" (qualified) and "Sapphire" (advanced) may differ under the application of law different to EU law and may be more or less extensive compared to EU law.

The exchange of encrypted data and the issuing of signature certificates is also subject to legal restrictions in/with certain states.

7.3 Data processing by third parties from home or abroad

Any data processing by third parties commissioned by Swisscom (Switzerland) Ltd. and/or from outside Switzerland is always carried out in accordance with the applicable provisions of the relevant legislation. Such processing may occur in particular if, for example, EU employees (cross-border commuters) or during business trips as well as by the maintenance divisions of EU manufacturers as well as by employees of Swisscom IT Services Finance S.E. in the role as trusted service provider. Within the framework of this service, the following constellations in particular are affected by processing of this kind:

- Swisscom IT Services Finance S.E. uses Swisscom (Switzerland) Ltd. to process the data required to provide its trust service, in particular for issuing electronic certificates.
- In the event of support cases from the EU, the 3rd level support of the application manufacturer has VPN access to application data at Swisscom (Switzerland) Ltd., which does not include any personal data other than the data published by the signatory in the signature certificate. This access is monitored by Swisscom (Switzerland) Ltd.. Identification data cannot be viewed by the application manufacturer.
- Supervisory authorities and conformity assessment authorities which have to confirm the conformity of the signature application for Swisscom IT Services Finance S.E. may come into contact with personal and identification data as part of audits under the supervision of Swisscom in order to assess the compliant implementation of identity verifications and the issuing of signatures.
- Identification data processed with the RA-App can also be collected abroad by the RA agent, depending on the situation.

If, during the provision of this service, Swisscom (Switzerland) Ltd. is confronted with outages that it is unable to resolve itself, it may grant manufacturers or service partners from the EU temporary and supervised VPN access to its systems for the purpose of analysing and rectifying faults. The signature data published by the signatory in the signature certificate and the master data of the customer organisation (e.g. organisation name, designation of the access certificate published by the Customer) may be visible to these third parties in individual cases. Access is monitored in real time by a Swisscom technician to ensure that there is no unsupervised access to data and that the connection can be severed immediately in the event of any misuse. This process corresponds to the best-practice approaches used in the banking and insurance sectors in Switzerland.