# Service description

## All-in Signing Service for advanced and regulated electronic seals Switzerland (Static Signatures)

# Table of contents

# 1 Service overview

The All-in Signing (AIS) service is a server-based remote signature service provided at the data centres of Swisscom (Switzerland) Ltd in Switzerland.

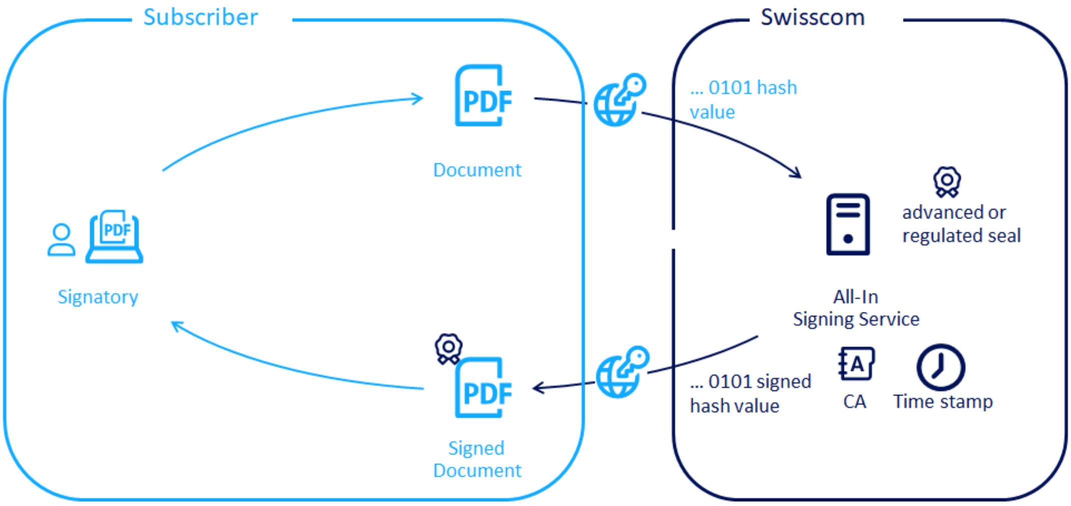
Swisscom (Switzerland) Ltd is a recognised provider of certification services in Switzerland for electronic signatures in accordance with the Swiss Federal Act on Electronic Signatures (ESigA) (Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur or "ZertES"). An accredited certification authority regularly checks whether the requirements imposed by Swiss law and/or technical norms on recognised providers of certification services for electronic signatures are met.

In general, AIS offers, depending on the type of contract, advanced and qualified electronic signatures for individuals as well as advanced and regulated electronic seals for organisations. This service description describes the service for advanced electronic seals and regulated electronic seals for organisations in accordance with Swiss law (ESigA).

Organisations that create seals (hereinafter "seal creators", see the detailed definition in section 2) can use AIS to attach an electronic seal to digital files, thereby ensuring the integrity and authenticity of a file. From a technical point of view, the electronic seal is based on the exact same procedure as the electronic signature. Swisscom (Switzerland) Ltd creates and manages the seal certificate for the seal creator on a fiduciary basis and makes it available for the AIS service through an encrypted channel. Thus, apart from a subscriber application, the seal creator does not need any other operational resources for this service, such as tokens or a signature card.

In the seal creation process, the subscriber application produces a document such that only the hash (check sum of fixed length without any indication of the content) is sent to the AIS service. The files that are effectively readable 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, thereby creating a signed document. All the hashes of the documents that are sent by the subscriber over the secure interface are signed by Swisscom. Batch operations are thus also possible. In this case, the subscriber agrees that the establishment of the authorised connection qualifies as approval to Swisscom for seal creation. The subscriber can also operate the subscriber application for a seal creator as a third party. In this case, Swisscom needs authorisation from the seal creator to create a seal via the subscriber application of the subscriber.

Before commencing the service, every seal creator submits a certificate application, which is verified by Swisscom or by a third party under the responsibility of Swisscom.

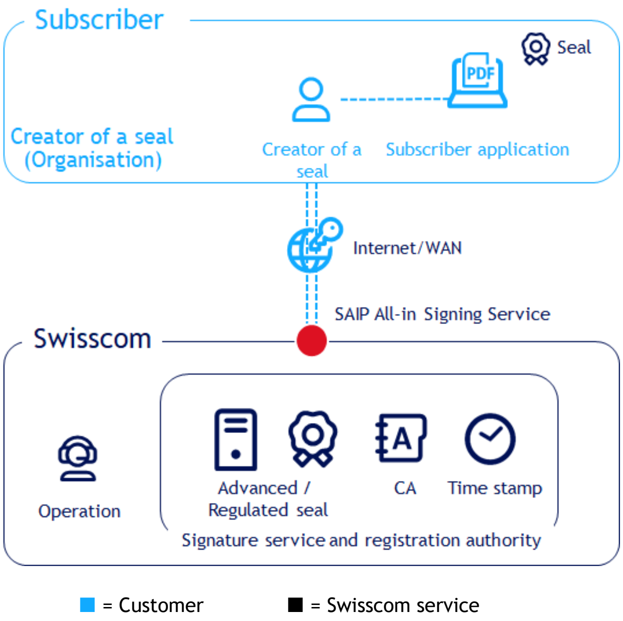


# 2 Definitions

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



## 2.2 Service-specific definitions

| Term | Description |
|---|---|
| Access certificate | Certificate that authenticates the access of the subscriber application to AIS and serves to encrypt communication with the AIS service. It is a publicly trusted SSL/TLS certificate or a SSL/TLS certificate that is signed by the subscriber and also includes the public key. The specification is included in the configuration and acceptance declaration.<br>If the subscriber and seal creator are identical, an authorised representative of the subscriber transmits the access certificate to Swisscom electronically (for example, by e-mail).<br>If the subscriber and seal creator are not identical, in addition to transmitting the access certificate to Swisscom, the written consent of the seal creator has to obtained allowing Swisscom to use the access certificate to create electronic seals in the name of the seal creator by means of the subscriber application of the subscriber. In the case of a regulated certificate, the seal creator always retains access to the private key of this access certificate and personally hands the certificate on to Swisscom. |
| AIS | All-in Signing |
| AIS service | All-in Signing service. The signature service provides an interface linked to a subscriber application to activate the seal creation. |
| BINA | Swiss Federal Act of 18 June 2010 on the Business Identification Number (Bundesgesetz vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer or “UIDG”) |
| CMS | Cryptographic message syntax – a syntax defined in RFC5652 for the digital signature and cryptographic messages. |
| CP/CPS | Certification guidelines (CP/CPS) for issuing certificates of the “Diamond” (qualified) and “Sapphire” (advanced) classes. |

All-in Signing service for electronic seals (CH)

B

| Term | Description |
|---|---|
| | Certification guidelines, certification practice and documentation of certification authorities defining the rules and standard practices for issuing certificates. |
| Distinguished name | Standard form for describing a certificate subject. The subject of a certificate unambiguously 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. |
| Electronic signature | The electronic signature is a technical procedure for verifying the authenticity of a document, an electronic message or other electronic data and the identity of the signatory. |
| Electronic seal | From a technical point of view, the electronic seal is based on the exact same procedure as the electronic signature.<br>An electronic seal is data in electronic form attached to other data in electronic form or logically linked to such data in order to ensure the origin and integrity of the data.<br>Under Swiss law, only regulated electronic seals for UID entities are regulated by law, not advanced electronic seals. |
| ESigA | 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”). |
| FIPS 140-2 | The Federal Information Processing Standard applies to published standards in the USA. |
| Hash | Unique representation of a large amount of data on a small amount of data, almost like a document’s fingerprint. No inferences can be made from the hash that would reveal the contents of the document in any way. |
| HSM | Hardware security module. This is a periphery device for the efficient and secure execution of cryptographic functions and applications, in particular for the protection of key information used cryptographically. |
| 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) |
| PKCS#1 | Cryptographic standard of the RSA Laboratories. |
| RA | **R**egistration **a**uthority |
| Registration authority (RA) | Authority responsible for the identification of future seal creators. May be provided by the subscriber, Swisscom or third parties, provided a contractual relationship with Swisscom exists. |
| REST | Representational state transfer. A programming paradigm for distributed systems, particularly web services. |
| Secure signature creation module (HSM) | Qualified and certified hardware for creating signature keys and signature certificates. |
| Signature | See “Electronic signature”. |
| Signature certificate or seal certificate | Certificate that is issued to the signer or the seal creator. It is managed by Swisscom on a fiduciary basis and is used for signature or seal creation. |
| Seal creator | Organisation (legal entity, administrative unit, etc.) that is a UID entity within the meaning of Article 3(1)(c) of the Swiss Federal Act of 18 June 2010 on the Business Identification Number (BINA) (Bundesgesetz vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer, UIDG), in whose name a digital certificate has been issued by Swisscom, on the basis of which it creates an advanced or qualified electronic seal.<br>Future seal creators must first apply to Swisscom for a digital certificate. Until the application has been approved by Swisscom, seal creators are applicants (who cannot create seals if the application is rejected). |

| Term | Description |
|---|---|
| SOAP | Simple Object Access Protocol – an interface programming paradigm for web services that represents an alternative to REST. |
| SSL/TLS | Secure Socket Layer/Transport Layer Security. Encryption protocols for secure data transmission on the Internet based on SSL/TLS (access) certificates. |
| Static signature | Term frequently used in technical documents for the “organisation signature” or “seal” in accordance with this service description. |
| Subscriber | Swisscom provides the services in accordance with this service description for the benefit of the subscriber. The subscriber is either a direct customer of Swisscom with an All-in Signing service contract (including the configuration and acceptance declaration) or has a commercial contract with a partner of Swisscom with a configuration and acceptance declaration with respect to Swisscom. Unless the subscriber is identical to the seal creator, the subscriber requires authorisation because the seal creator sends or transfers the access certificate to Swisscom electronically or accepts the access certificate authorised by the subscriber for Swisscom. |
| Subscriber application | The subscriber provides one or more seal creators with access to an application with which they can create electronic seals in accordance with Swisscom’s terms and conditions of use, and the subscriber ensures not only the authentication but also the transmission of the seal data to the remote signature service of Swisscom. The subscriber application receives the signed data and prepares the document for the seal creator.<br>The subscriber application is not part of this service description. It is provided outside of the AIS service, for example, by partners of Swisscom. |
| Terms and conditions of use | The terms and conditions of use govern the use of the seal certificates and certification service in the relationship between Swisscom (Switzerland) Ltd and the seal creator on a subscriber application. They can be viewed at https://www.swisscom.ch/en/business/enterprise/offer/security/digital_certificate_service.html. |
| UID entity | Organisation in accordance with Article 3(1)(c) BINA that is assigned a business identification number for unique identification.<br>Only UID entities may be creators of electronic seals pursuant to CP/CPS. |

# 3 Variants and options

| Standard variant | Electronic seal |
|---|---|
| Advanced electronic seal | ● |
| Regulated electronic seal | ● |
| Qualified electronic time stamp | ● |
| Data storage in Switzerland | ● |
| Operation in accordance with certification guidelines (CP/CPS) | ● |

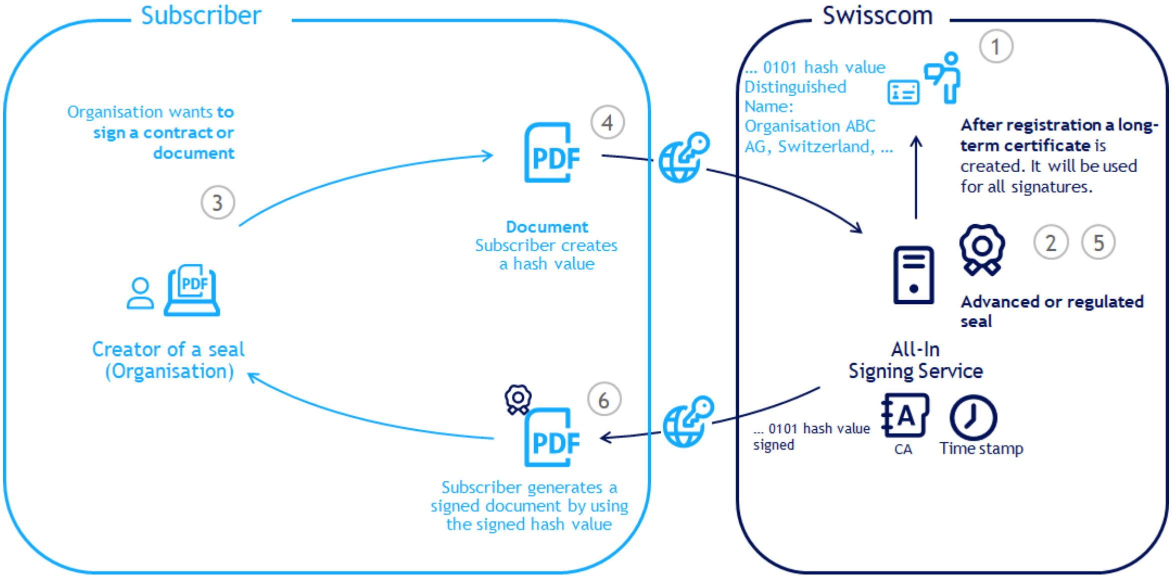
● = Standard (included in the price)

## 3.1 Definition of the service performances and options

| Performance/Option | Definition |
|---|---|
| Advanced electronic seal | Advanced electronic seal in accordance with ETSI Standard 319 411 “NCP+”. |
| Regulated electronic seal | Regulated electronic seal in accordance with Article 2(d) ESigA: an advanced electronic signature created using a secure seal creation module pursuant to Article 6 ESigA on the basis of a regulated certificate valid at the time the electronic seal was generated. Seal certificates can only be issued in the name of a UID entity. |
| Qualified electronic time stamp | Qualified electronic time stamp in accordance with Article 2(j) ESigA. |

| Performance/Option | Definition |
|---|---|
| Data storage in Switzerland | Personal data associated with the certificates is stored exclusively in Switzerland in compliance with the applicable provisions of Swiss data protection law. |
| Operation in accordance with certification guidelines (CP/CPS) | The operations of certification service providers are governed by the certification guidelines (CP/CPS) of Swisscom (Switzerland) Ltd on the issue of seal certificates.<br>The latest version can be viewed here:<br>https://www.swisscom.ch/en/business/enterprise/offer/security/digital_certificate_service.html<br>Regulated electronic seals are based on regulated certificates ("Diamond" class). Advanced seals are based on certificates of the "Sapphire" class. |

## 3.2 Seal creation procedure


Subscriber
Organisation wants to sign a contract or document
3
Creator of a seal (Organisation)
4
Document
Subscriber creates a hash value
6
Subscriber generates a signed document by using the signed hash value
Swisscom
... 0101 hash value
Distinguished Name:
Organisation ABC AG, Switzerland, ...
1
After registration a long-term certificate is created. It will be used for all signatures.
2
5
Advanced or regulated seal
All-In Signing Service
... 0101 hash value signed
CA
Time stamp

- The registration authority (1) authenticates the seal creator beforehand on the basis of register entries and accepts an application from an authorised representative of the seal creator. The latter must appear in person before a representative appointed by Swisscom. The application and other documents submitted are checked and archived.
- After the application has been approved, the key material is created and stored for the seal creator on the AIS platform (2). A corresponding long-term certificate (usually three years) is issued for this key pair in accordance with the certification guidelines of Swisscom and with the subject of the seal certificate in the seal certificate application (distinguished name of the seal creator).
- The subscriber authorised by the seal creator or the seal creator itself issues an SSL/TLS access certificate. The subscriber saves this on its server. In addition, the subscriber sends a copy of this access certificate to Swisscom, which saves it on the AIS platform. This ensures the connection between the subscriber application and the AIS service.
- In the case of regulated electronic seals, the private key of the access certificate must be created and managed on a cryptographic module or HSM with a minimum standard of FIPS 140-2 that has been agreed with Swisscom or its partner (such as Yubikey FIPS Series authentication devices). The private key is created by the subscriber with the cryptographic module or HSM in the presence of a representative appointed by Swisscom.
- All signature applications are also authenticated with this access certificate; other individual authentication no longer applies.
- The seal creator selects the document (3) or set of documents to be signed. The subscriber application creates a hash in accordance with Swisscom provisions (4) and sends it to the AIS service. Information relevant to the seal certificate subject (distinguished name) is also sent by the subscriber application.

- If the distinguished name of the seal creator is recorded by the registration authority and authorised for the creation of seals, a hash signature (5) is generated in accordance with CMS or PKCS#1 standard to ensure the integrity of the hash.
- The seal with additional validation information in the signature certificate (such as signature certificate chain for a trustworthy root certificate and qualified time stamp) is returned. The subscriber application ensures the seal of the document by embedding the signed hash in the document. (6)
- The security of the subscriber application is ensured through regular self-audits by the subscriber in accordance with the configuration and acceptance declaration and, if needed, through an audit by Swisscom.

### 3.3 Process for authenticating a seal creator

Before the service commences, Swisscom conducts an audit of the seal creator in accordance with the provisions of CP/CPS (see above). For this purpose, the seal creator must be named in the seal certificate application and a representative who is an authorised signatory of the seal creator must sign the application for a seal certificate. In the case of signature regulations calling for two authorised signatories, another representative of the seal creator must also sign. By signing the seal certificate application, the seal creator authorises Swisscom to issue the certificate. The signatures must take place in the presence of an authorised representative of Swisscom either as a qualified electronic signature or by hand.

### 3.4 Revocation (declaration of invalidity) of a seal certificate

Seal certificates and/or access certificates must be declared invalid by the seal creator if there are visible signs that they have been misused or compromised. Swisscom will then issue a new seal certificate, if necessary on the basis of a new access certificate.

A notice of revocation must be issued by the representative of the seal creator named in the certificate application whose means of authentication (mobile number) has been stored at Swisscom. A revocation request is verified by means of the stored mobile number and release. Other procedures for revocation are possible in accordance with the provisions of CP/CPS.

# 4 Service provision and responsibilities

## Non-recurring services

| Activities (S = Swisscom/Su = Subscriber) | S | Su |
|---|---|---|
| **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. 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 the signed configuration and acceptance declaration with activation-relevant information and the required contact persons. | | ✓ |
| 4. Implementation of the requirements of the configuration and acceptance declaration. | | ✓ |
| 5. Provision of an application for a seal certificate signed by the seal creator with all the necessary documents for authenticating the seal creator (e.g. certified extract from the commercial register for a regulated seal) and consent to the terms and conditions of use of the service. Signature in the application for the seal certificate by an authorised representative of the seal creator. Identification obtained through the personal appearance of a representative of the seal creator or through a qualified electronic signature. | | ✓ |
| 6. Assurance that an access certificate is sent to Swisscom by the seal creator or its authorised representative with confirmation of power of attorney in the signed acceptance and configuration declaration. | | ✓ |
| 7. Creation and management of the private key for the access certificate in a Swisscom approved storage solution or HSM with minimum FIPS 140-2 certification by the seal creator or authorised partner, insofar as qualified electronic seals are created. If no process approved by Swisscom exists, the private key is generated on the authorized storage solution or HSM in the presence of an authorised representative of Swisscom and the | | ✓ |

| Activities (S = Swisscom/Su = Subscriber) | S | Su |
|---|---|---|
| customer's representatives named and authorised in the seal application form. In this case, the creation and transmission of the access certificate are recorded in a jointly signed protocol. | | |
| 8. Activation of the communication for the access certificate sent. | ✓ | |
| 9. If required, configuration of the firewall, on the server side at the subscriber. | | ✓ |
| 10. Designation of a person responsible, including constant deputation, for all matters concerning technology and security and contact partners for audit matters in the configuration and acceptance declaration. | | ✓ |
| 11. Review of application documents. | ✓ | |
| 12. Connection of the subscriber and sending of subscriber-specific access data. | ✓ | |
| 13. Integration of the AIS service into the subscriber-specific application(s) and/or subscriber-side connection of the interface to AIS, e.g. through the use of a subscriber application of a partner. | | ✓ |
| 14. Verification of access to the AIS service and the information on the seal certificate. Immediate report of any errors to Swisscom before being used for seal creation. | | ✓ |
| 15. Fault rectification through update or re-installation. | ✓ | |
| 16. Operation of a revocation office for declarations of invalidity of a seal certificate if the seal certificate has been compromised or for other reasons. | ✓ | |
| 17. Revoking and enabling of revocations by the seal creator if there are signs that the seal or access certificate has been compromised through a revocation process published by Swisscom. | | ✓ |
| 18. Notification of the relinquishment of business activities, a bankruptcy notice against the subscriber, the opening of bankruptcy proceedings or a debt restructuring moratorium. | | ✓ |

| Termination of the service or termination of the seal creation for a seal creator | | |
|---|---|---|
| 1. Deletion of the seal and access certificates in the AIS infrastructure. | ✓ | |
| 2. Deletion of the associated key from the HSM. | ✓ | |

## Recurring services

| Activities (S = Swisscom/Su = Subscriber) | S | Su |
|---|---|---|
| **Standard services** | | |
| 1. Operation of the AIS infrastructure, renewal of the seal certificate before its validity expires. | ✓ | |
| 2. Lifecycle management of the AIS service infrastructure. | ✓ | |
| 3. Lifecycle management of the subscriber’s infrastructure: updating to the current status of technology and security (security patches, updates, etc.). | | ✓ |
| 4. Appropriate technical and organisational measures to protect the data sent from the subscriber application (e.g. including through the deactivation of connections not required or access regulations, etc.). Disclosure of the security system of the subscriber application and communication to Swisscom, if so requested by Swisscom or its certification authority. | | ✓ |
| 5. Amendment of the definition of the security requirements. | ✓ | |
| 6. Lifecycle management of the access certificate: timely exchange before expiration of validity by the seal creator itself by e-mail to 1st-level support of Swisscom, specifying the claimed identity and the PRO number named in the contract. | | ✓ |
| 7. Assurance of the confidentiality of the data exchange between Swisscom and the subscriber (for example, avoidance of “inspection” modules). | | ✓ |

| Activities (S = Swisscom/Su = Subscriber) | S | Su |
|---|---|---|
| 8. Selection of an approved storage solution or HSM in the case of a regulated seal that allows access to the subscriber application to be blocked at the latest after 5 failed attempts at authentication to the service. A new access certificate must then be issued in accordance with the authorised process or in a joint ceremony with Swisscom. | | ✓ |
| 9. Creation of seal certificates. | ✓ | |
| 10. Definition of the seal certificate content and procedure for seal creation. | ✓ | |
| 11. Sending of the seal creator's data (distinguished name) in accordance with the provisions of the certificate application of the seal creator and the configuration and acceptance declaration. | | ✓ |
| 12. Creation of seals. | ✓ | |
| 13. Creation of seals in conjunction with a qualified time stamp in accordance with ESigA. | ✓ | |
| 14. Fulfilment of the cooperation obligations and requirements by the security officer. | | ✓ |
| 15. Customer notification in the event of outages and maintenance. | ✓ | |
| 16. Provision of support services (service desk, incident management, etc.). | ✓ | |
| 17. Reporting of changes to subscriber-specific information (contact persons, access certificate, termination of seal creation, etc.). | | ✓ |
| 18. Updating of subscriber-specific information (contact persons, access certificate, etc.). | ✓ | |
| 19. Reporting of service faults. | ✓ | |
| 20. Reporting of any security incident on the system of the subscriber application which concerns the AIS service. | | ✓ |
| 21. Reporting of any security incident on the system of the signature service which impacts the subscriber or seal creator. | ✓ | |
| 22. Further development, adjustment of the interface to current regulatory and security requirements. Information on adjustment of the interface three months before release, unless immediate action is called for by law or for security reasons. Maximum of two adjustments per year. | ✓ | |
| 23. Adjustment of the interface in line with Swisscom's new requirements within three months. | | ✓ |

# 5 Service levels and reporting

## 5.1 Service levels

The following service levels generally relate to the agreed support time. 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. In the case of several possible service levels per variant, the service level is selected in the service contract.

| Service level & targets | | | Electronic seal |
|---|---|---|---|
| **Operation Time** | | | |
| Operation Time | Mo-Su | 00:00-24:00 | |
| Provider Maintenance Window | PMW-DC | PMW Data Centre Swisscom | ● |
| | PMW-S:<br>with advance notice for security and system-critical updates | Daily<br>19:00-07:00, for announced maintenance only | ● |

| Service level & targets | | | Electronic seal |
|---|---|---|---|
| **Support Time** | | | |
| Support Time | Mo-Fr | 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 2.2 | 99.9% | | ● |
| **Security** | | | |
| | Advanced (ITSLA) | | ● |
| | Customised (ITSLC) | | ○ |
| **Continuity** | | | |
| ICT Service Continuity (ICTSC)[1] | 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 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 Customer’s requirements.

| Service level report | | Electronic seal | Reporting period |
|---|---|---|---|
| Availability | Service availability | | |
| | ▪ Signature service | ● (On request) | Monthly |
| | ▪ Directory services | ● (On request) | Monthly |

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

## 6 Billing and quantity report

### 6.1 Billing

Services are billed retroactively for the previous month. The billing details are set out in the service contract.

[1] RTO and RPO only concern the provision of the AIS service on SAIP. Mobile services used for the identification, authentication or declaration of consent are not included here.

### 6.2 Quantity report

Quantity reports are governed by the service contract.

## 7 Special provisions

### 7.1 Subscriber application

The subscriber application is not part of this service description. The subscriber application is provided by the subscriber, by a Swisscom partner or by Swisscom.

### 7.2 Operation of the subscriber application if the subscriber and seal creator are not identical

The representative of the seal creator authorised in the certificate application must transfer the access certificate to Swisscom or, in the case of advanced seals, approve the transfer of the access certificate to Swisscom by the subscriber in writing. This authorises the subscriber to operate the subscriber application for the seal creator with respect to Swisscom. If the authorised representative changes, Swisscom is to be notified in writing or by e-mail by a representative of the seal creator or by the previous contact.

In this way, all documents that are transmitted via the Swisscom interface will have an electronic seal. Swisscom cannot verify that the access of the operator of the subscriber application with authority to access the key material for seal creation was authorised or that it was error-free.

### 7.3 Potential applications of the advanced or regulated electronic seal

The use of the advanced or regulated electronic seal generally serves to guarantee the proof of origin and the integrity of the content of a file. The electronic seal is not to be confused with the legal concept of the electronic signature. Moreover, the legal effects of the higher-quality regulated electronic seal are not the same as those for the advanced electronic seal. It is up to the subscriber and the subscriber's seal creator to clarify in advance the legal effects of the chosen type of electronic seal (with or without a time stamp). Swisscom accepts no responsibility in this regard.

Regulated electronic seal (based on a certificate of the Swisscom "Diamond" class): the regulated seal created using AIS satisfies the criteria defined in the CP/CPS and the definition in accordance with Article 2(d) of the Swiss Federal Act on Electronic Signatures (ESigA; SR 943.03).

Advanced electronic seal (certificate of the Swisscom "Sapphire" class): the advanced electronic seal created using AIS satisfies the criteria defined in the CP/CPS and, in contrast to the regulated electronic seal, is not regulated by law.

Qualified electronic time stamp: the qualified electronic time stamp created using AIS satisfies the criteria defined in the CP/CPS and the definition in accordance with Article 2(j) ESigA.

The advanced electronic seal and the regulated electronic seal do not have the same legal effects as a handwritten signature or a qualified electronic signature. Depending on the situation, some documents therefore require a handwritten signature, a qualified electronic signature or a regulated electronic seal, under certain circumstances with an electronic time stamp, in order for the intended legal validity to enter into effect.

In the event that foreign law is applicable, electronic seals issued using AIS may have legal effects that differ from, exceed or fall short of those under Swiss law.

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

### 7.4 Data processing by third parties in Switzerland or abroad, emergency access

Data transmitted to Swisscom by the subscriber (seal creation data) within the scope of service provision are generally processed by Swisscom in Switzerland. Any data processing by third parties commissioned by Swisscom and/or from abroad is always carried out in accordance with the applicable provisions of Swiss data protection law. Such processing may occur, in particular, in instances in which the data are processed by employees domiciled in the EU (cross-border commuters) or while travelling as well as in cases where data are handled by the maintenance divisions of manufacturers from the EU. Within the framework of this service, the following constellations may specifically be affected by such processing:

- In support cases, the 3rd-level support of the application manufacturer has VPN access from the EU to the Swisscom network with application data that do not include any personal data. This access is monitored by Swisscom. 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 may come into contact with personal and identification data as part of audits under the supervision of Swisscom conducted in order to assess the compliant implementation of identity authentication and the issuing of signatures. These compliance assessments only take place in Switzerland.

If, during the provision of this service, Swisscom is confronted with faults that it is unable to resolve itself, it may grant manufacturers or service partners from the EU temporary, supervised VPN access to the systems of Swisscom for the purpose of fault analysis and rectification. The signature data disclosed by the seal creator in the certificate and the master data of the seal creator (e.g. organisation name, designation of the access certificate published by the Customer) may also be visible to these third parties in some 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 is consistent with the best-practice approaches used in the banking and insurance sectors.