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

Service Description
Signing Service for qualified electronic time stamp according to ESigA (ZertES) and eIDAS regulation

Swisscom Trust Services

Swisscom Trust Services AG

Hardturmstr. 3
8005 Zürich

Switzerland

https://trustservices.swisscom.com
E-Mail: sts.salessupport@swisscom.com

1 Content

2 Service overview

The Signing Service 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" and Swisscom (Switzerland) Ltd. and offered by Swisscom Trust Services Ltd., Switzerland. The Signing Service is provided in the data centres of Swisscom (Switzerland) Ltd. in Switzerland and Swisscom Trust Services Ltd. (hereafter “Swisscom”) distributes the Signing Service in its own name or grants third parties the right to distribute the Signing Service in its own name.

The remote signature service is made available to subscribers operating a subscriber application. Swisscom (Switzerland) Ltd generates the timestamp and operates the service and manages the time stamp certificate. Swisscom (Switzerland) Ltd as subcontractor is responsible for the trusted service of the subsidiary Swisscom ITSF. The signature service will be provided via a secured channel to the subscriber application. The signatory or timestamp creator needs a signature application as subscriber application which timestamps the document.

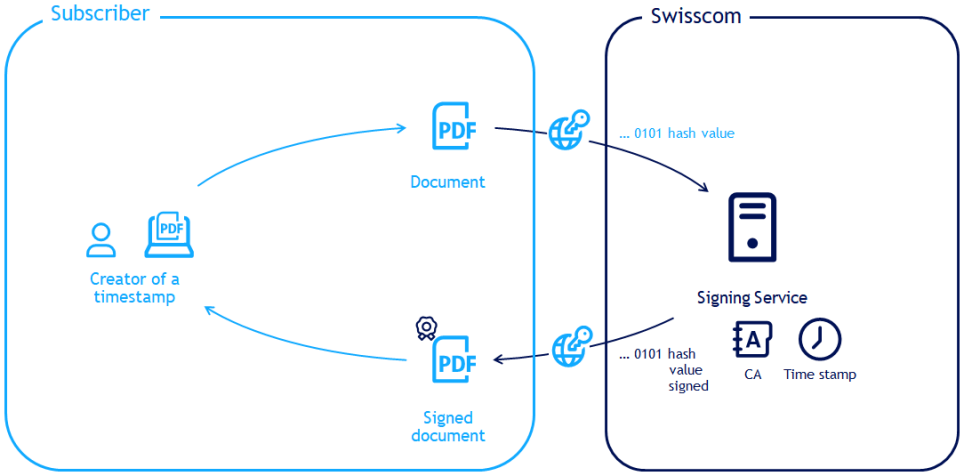
Swisscom (Switzerland) Ltd is a recognised provider of certification services in Switzerland for electronic signatures in accordance with the Swiss Electronic Signatures Act (ESigA (ZertES); SR 943.03). An accredited certification authority regularly checks whether the requirements imposed by Swiss law and/or technical norms on recognised providers of certification services for electronic signatures are met.

Swisscom ITSF is recognised for issuing qualified certificates for electronic signatures, electronic seals and qualified time stamps in accordance with the eIDAS Regulation and the Austrian Signature and Trust Services Act (SVG). A conformity assessment body regularly checks whether the requirements imposed by EU and Austrian law and/or technical norms on trusted service providers are met. The supervisory authority granted Swisscom ITSF qualification status as a qualified trust service provider.

In general, Signing Service 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 qualified electronic time-stamp service. Qualified time stamps according to this service description comply with the definition of Art. 2 letter j ESigA and under EU law the definition of Art. 3 para. 34 eIDAS regulation.

Subscribers using the service can use Signing Service to attach a qualified electronic time stamp to digital files, thereby ensuring the integrity and the time at which the stamp was placed on a file. From a technical point of view, the qualified electronic time stamp is based on exactly the same procedure as the electronic signature. Swisscom (Switzerland) Ltd or Swisscom ITSF creates and manages the time-stamp certificate and makes it available for the Signing Service through an encrypted channel.

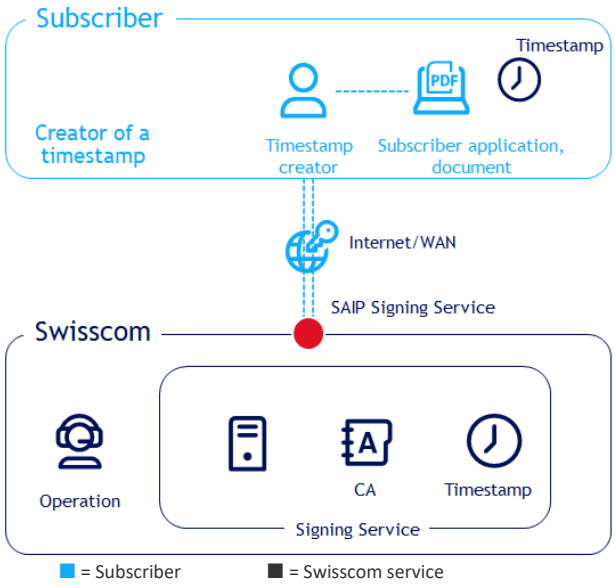
In the time-stamp-creation process, the subscriber application produces a document such that only the hash (check sum of fixed length without any indication of the content) is sent to the Signing Service. The files that are effectively readable and the information they contain do not leave the subscriber’s system environment and cannot, therefore, be viewed by Swisscom. The time-stamped hash is reintegrated into the document by the subscriber application, thereby creating a time-stamped document. All the hashes of the documents sent by the subscriber over the secure interface are time-stamped by Swisscom, thereby also enabling batch operations. The subscriber can also operate the subscriber application for a third party. No authorisation is required for this since the qualified electronic time stamp does not include any user information whatsoever.



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 levels are reported.
The SAIP is the interface that receives requests from the subscriber application and answers them according to the Reference Guide (**http://documents.swisscom.com/product/1000255-Digital_Signing_Service/Documents/Reference_Guide/Reference_Guide-All-in-Signing-Service-en.pdf**). The response can also be a documented error message.
The following schematic diagram serves to illustrate the services and service components of the Signing service:



3.2 Service-specific definitions

Term	Description
Declaration of acceptance	The subscriber signs a declaration of acceptance that specifies the subscriber's obligations, such as the creation of SSL certificates or virus protection.
Access certificate	Certificate that authenticates the access of the subscriber application to Signing Service and enables encrypted communication with the Signing Service. It is a publicly trusted SSL/TLS certificate or an SSL/TLS certificate that is signed by the subscriber and also includes the public key. The specification is included in the declaration of acceptance.
CP/CPS	Certification guidelines (CP/CPS) for issuing certificates of the "Diamond" (qualified) and "Sapphire" (advanced) classes. Certification guidelines, certification practice and documentation of certification authorities defining the rules and standard practices for issuing certificates.
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 the repeal of Directive 1999/93/EC); also regulates the electronic signature and time stamps.
Electronic seal	From a technical point of view, the electronic seal is based on exactly the same procedure as the electronic signature. 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. Under Swiss law, only regulated electronic seals for BIN (UID) entities are regulated by law, not advanced electronic seals.

Term	Description
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 timestamp	A timestamp certifies that electronic data was present to the creator of the timestamp at the specified time and date.
ESigA	See ZertES
ETSI	European Telecommunications Standards Institute
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.
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).
REST	Representational state transfer. A programming paradigm for distributed systems, particularly web services.
RFC 3161	Internet standard for a Time-Stamp Protocol
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.
Signing Service	The signature service provides an interface linked to a subscriber application to trigger time-stamp creation.
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.
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 a Signing Service contract (including the declaration of acceptance) or has a commercial contract with a reseller of Swisscom's services with a declaration of acceptance with respect to Swisscom.
Subscriber application	The subscriber provides one or more signatories with access to an application with which they can create qualified electronic time stamps in accordance with Swisscom's terms and conditions of use, and the subscriber ensures the secure transmission of the document's data to the remote signature service of Swisscom. The subscriber application receives the time-stamped data and prepares the document for the timestamp creator. The subscriber application is not part of this service description. It is provided outside of the Signing Service, for example, by partners of Swisscom.
Terms and conditions of use	The terms and conditions of use govern the use of the timestamp certificates and certification service in the relationship between Swisscom (Switzerland) Ltd and the timestamp creator on a subscriber application. They can be viewed at **https://trustservices.swisscom.com/repository/**
Time Stamp Policies	A certificate authority document that describes the policies and practices for issuing time stamps.
Timestamp certificate	General certificate, which is not assigned to a user and serves to issue a time stamp.
ZertES/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 "ESigA").

4 Variants and options

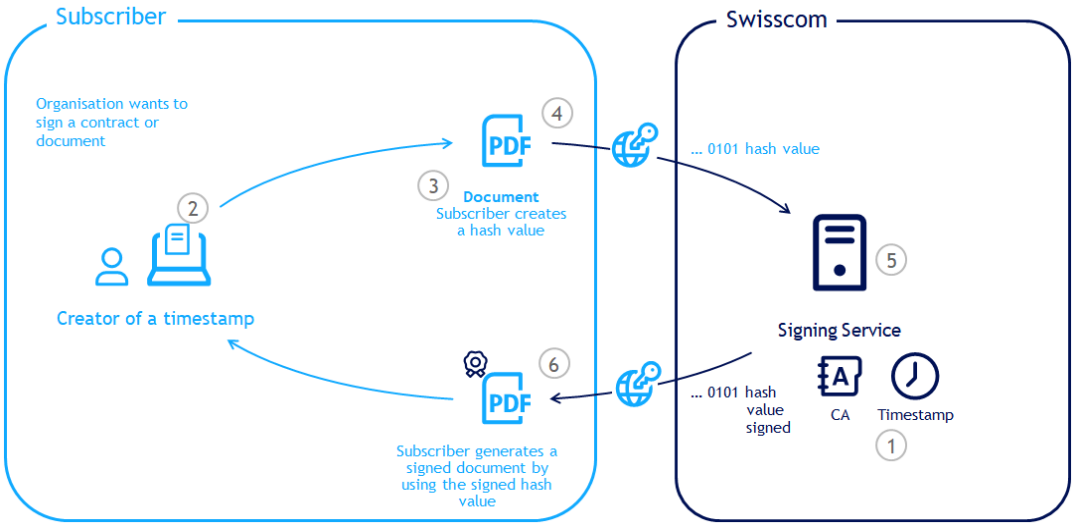
Standard variant	Signing service Time stamp
Qualified electronic time stamp	●
Operation in accordance with Time Stamp Policies	●

● = Standard (included in the price)

4.1 Definition of the service specification

Service variant	Definition
Qualified electronic time stamp	Qualified electronic time stamp in accordance with Article 2(j) ESigA and with Art. 3 para. 34 eIDAS regulation
Operation in accordance with Time Stamp Policies	The operations of certification service providers are governed by the Time Stamp Policies ("TSA Policies") on the issue of time stamps of Swisscom (Switzerland) Ltd or Swisscom ITSF. The latest version can be viewed here: **https://trustservices.swisscom.com/repository/** Time-stamp certificates are based on "Diamond" class certificates.

4.2 Time-stamp-creation procedure



- Swisscom saves time-stamp certificate on its platform in a secure signature creation module (1).
- The subscriber creates an SSL/TLS access certificate and saves it on his/her server. In addition, the subscriber sends a copy of this access certificate to Swisscom, which saves it on the Signing Service platform. This ensures the connection for all time-stamp jobs between the subscriber application and the Signing Service.
- The Creator of a timestamp (2) 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 Signing Service.
- A qualified electronic time stamp from a time-stamp service set up in accordance with RFC3161 is attached to the hash (5).
- The hash with the qualified electronic time stamp is returned along with additional validation information in the time-stamp certificate (such as signature certification chain for a trustworthy root certificate and revocation

information). The subscriber application safeguards the document's qualified electronic time stamp by embedding the time-stamped hash into the document. (6)

- The security of the subscriber application is ensured through regular self-audits of the subscriber in accordance with the declaration of acceptance and, if needed, through an audit by Swisscom (performed by Swisscom itself or a third party commissioned by Swisscom).

4.3 Process for authenticating a subscriber application

Before the service commences, Swisscom authenticates the subscriber application in accordance with the provisions of CP/CPS (see above). For this, the subscriber must sign declaration of acceptance that specifies the subscriber's obligations, such as the creation of SSL certificates.

4.4 Standards used

The OASIS DSS protocol is used (signature type "urn:ietf:rfc:3161"), which can be called via a REST API or SOAP API. The time stamp is based on ETSI 319 422 and is geared toward the structure in the RFC 3161 protocol. The RFC 3161 protocol is not supported externally.

5 Service provision and responsibilities

Non-recurring services

Activities (S = STS/Su = Subscriber)		S	Su
Provisioning of service			
1.	Provision of the Signing Service 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 declaration of acceptance with activation-relevant information and the required contact persons.		✓
4.	Implementation of the requirements of the declaration of acceptance including the acceptance of the terms of use.		✓
5.	Assurance that an access certificate is sent to Swisscom.		✓
6.	Activation of the communication for the access certificate sent.	✓	
7.	Integration of the Signing Service into subscriber-specific application(s) and/or subscriber-side connection of the interface to Signing Service, e.g. through the use of a partner's subscriber application.		✓
8.	Verification of access to the Signing Service and the information contained in the qualified electronic time stamp. Immediate notification of any errors to Swisscom before the time stamp is used productively outside these error tests.		✓
9.	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 timestamp creation			
1.	Deletion of access certificates in the Signing Service infrastructure.	✓	

Recurring services

Activities (**S = STS/Su = Subscriber**)		S	Su
Standard services			
1.	Operation of the Signing Service infrastructure, renewal of the timestamp certificate before its validity expires, operation of a revocation office that can declare a time-stamp certificate invalid in the event that it is compromised.	✓	
2.	Lifecycle management of the subscriber's infrastructure: updating to the current status of technology and security (security patches, updates etc.).		✓
3.	Amendment of the definition of the security requirements.	✓	

Activities (**S = STS/Su = Subscriber**)		**S**	**Su**
4.	Lifecycle management of the access certificate: timely exchange before expiration of validity by the timestamp creator itself by e-mail to Swisscom's 1st-level support, specifying the claimed identity and the PRO number given in the contract.		✓
5.	Assurance of the confidentiality of the data exchange between Swisscom and the subscriber (for example, avoidance of "inspection" modules).		✓
6.	Creation of qualified electronic time stamps.	✓	
7.	Subscriber notification in the event of faults and maintenance.	✓	
8.	Provision of support services (service desk, incident management, etc.).	✓	
9.	Reporting of changes to subscriber-specific information (contact persons, access certificate, end of need for time stamps, etc.).		✓
10.	Updating of subscriber-specific information (contact persons, access certificate, etc.).	✓	
11.	Reporting of service faults.	✓	
12.	Immediate notification of any security incidents on the system used for the subscriber application that concerns the Signing Service.		✓
13.	Reporting of security incidents on the system used by the signature service that has an impact on subscribers.	✓	
14.	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.	✓	
15.	Adjustment of the interface in line with Swisscom's new requirements within three months.		✓

6 Service levels and reporting

6.1 Service levels

The following service levels generally relate to the agreed monitored operation times. Definitions of terms (Operation Time, Monitored Operation Time, Support Time, Availability, Security and Continuity) and the description of the measurement method and reporting are set out in the contractual element "Base Document".
The following service levels are provided for the service variants (see section 3). If several possible service levels are available for each variant, the service level is selected in the service contract.

Service level and target values			**Signing Service Electronic timestamp**
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	●

[1] If the Signing Service was supplied by a Swisscom partner, the latter 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] For public holidays, see the "SLA definitions" basic document.

Service level and target values		Signing Service Electronic timestamp
Availability		
Service Availability		
Signature service	99.9%	●
Directory services according to CP/CPS section 2.2	99.9%	●
Security		
	See base document	●
Continuity		
Service Continuity (STSSC)[3]	RTO 24 h | RPO 24 h	●

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

6.2 Service level reporting

On request a Service Level Report is available showing the availability of a dedicated months.

7 Billing and quantity report

7.1 Billing

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

7.2 Quantity report

Quantity is indicated on the service bill.

8 Special provisions

8.1 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 in accordance with a separate agreement.

8.2 Possible uses of qualified electronic time stamps

A qualified electronic time stamp is usually used to certify that a document existed in a certain form at a certain time and should not be confused with the legal concept of the electronic signature or electronic seal. It is up to the subscriber and the subscriber's timestamp creators to clarify in advance the legal implications of the qualified electronic time stamp. Swisscom shall accept no responsibility in this regard.
The qualified electronic time stamp created using Signing Service satisfies the criteria defined in the CP/CPS and the definition in accordance with Article 2(j) ESigA or article 3 (34) eIDAS regulation
In the event that foreign law is applicable (other than ZertES for Switzerland and eIDAS regulation for EU), time stamps issued using Signing Service may have legal effects that differ from, exceed or fall short of those under Swiss or EU law. The exchange of encrypted data and the issuing of certificates in/with certain states are also subject to legal restrictions.

8.3 Data processing

Hash values transmitted to Swisscom by the subscriber within the scope of service provision are generally processed by Swisscom in Switzerland. No personal data are processed in connection with time-tamp creation.

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