SwissSign

SwissSign Terms and Conditions of Use for qualified electronic signature and simple electronic signature

1. Applicability

These Terms and Conditions of Use shall apply in the relationship between the End User and SwissSign AG, Sägereistrasse 25, 8152 Glattbrugg (hereafter: "SwissSign") in connection with the use of a SwissSign Signing Service and the corresponding certification services for the electronic signature (hereafter: "Signing Service").

The Terms and Conditions of Use shall be displayed to the End User at the time of the electronic order for the Signing Service. The End User must expressly accept the Terms and Conditions of Use. The Terms and Conditions of Use, which form an integral component of the Agreement, are also published on the website https://www.swissid.ch/en/sign/tnc.

2. Service

SwissSign offers the End User the option of signing documents using an electronic signature, which may be either a qualified electronic signature or – for business customers who have concluded a corresponding agreement – a simple electronic signature.

2.1 Qualified electronic signature

The services in connection with qualified electronic signatures under Art. 2(e) of the Swiss Federal Act on Electronic Signature (ESigA, SR 943.03) shall be provided in accordance with the relevant applicable Certificate Policies. These form an integral part of these Terms and Conditions of Use.

You can find the current Policies, in particular also the Relying Party Agreement (RPA) at the following link:

https://www.swisssign.com/en/support/repository

SwissSign is a provider of certification services recognised in Switzerland with qualified certificates in accordance with the ESigA. SwissSign shall be regularly checked by the accredited recognition authority for compliance with the ESigA.

SwissSign shall issue a signature certificate containing information on an identified person. The certificate makes it possible to affix qualified electronic signatures to documents such as in the form of PDF files. The signature can be uniquely assigned to the identified person based on the signature certificate and can also be validated by third parties. Any use of the signature certificates other than that described above is not permitted.

2.1.1 Identification of signatories

SwissSign or the Registration Authority (RA) appointed by it checks the identity of the End User in the identity verification process.

In the case of a qualified electronic signature, the identity of the End User is verified in a face-to-face meeting using his or her passport or an identity card recognised in Switzerland, and the identity document is checked for authenticity and validity.

For the issuance of certificates, End Users may be identified using a process equivalent to a face-to-face meeting.

SwissSign or the RA appointed by it files the personal information which is collected in the identity verification process in accordance with the applicable regulations.

2.1.2 Signature creation

Provided all requirements are met, SwissSign creates a personal certificate and the corresponding private cryptographic key on the Hardware Security Module (HSM) for the purpose of creating the signature. Only the End User has the activation data with which he can use the private key after authentication through an authentication method linked to his ID. Certificates are only issued when the subscriber attempts to perform a signature. This step is sufficient, and no further confirmation is required for certificate acceptance. Only if the activation data is entered, a qualified electronic signature is created.

2.1.3 Verification of the qualified electronic signature's validity

The validity of the electronic signature may be verified by the End User or third parties.

Verification is possible e.g. on the website www.validiator.ch or directly in Adobe Acrobat, a software application developed by Adobe Systems Inc.

2.2 Simple electronic signature

Simple electronic signature is based on a certificate which is issued in the name of a legal entity, which is ordinarily SwissSign AG. For this reason, personal identification of the End User is not required for the use of these signatures.

Simple electronic signature may be used where the following prerequisites are met: The End User has access to the email address which he uses to access the SwissID Sign service.

In addition, a corresponding contractual agreement with SwissSign is required.

2.3 System availability

SwissSign endeavours to ensure that the Signing Service operates as continuously as possible. SwissSign assumes no liability for the continuous availability of the Signing Service. SwissSign may temporarily restrict availability to carry out maintenance and repairs, as well as measures to improve the service or to ensure security and integrity. Wherever possible, maintenance work or other measures shall be performed outside normal usage hours.

3. Requirements for using the service

The End User is aware of the use and legal consequences of digital signature certificates pursuant to the ESigA. He must have access to an internet portal or business application that uses the Signing Service provided by SwissSign. He must also have a user account at the necessary security level for using the Signing Service. In addition, a secure means of authentication for triggering the signing process, such as a smartphone with iOS 12.0 or later or Android 9.0 or later (including fingerprint scanner / facial identifier and secure element) is also required in order to use qualified electronic signatures. Additional provisions that may restrict the use of the Signing Service are set out in the terms and

conditions of the business customer's applications that use the Signing Service.

The End User is particularly aware that the SwissSign services are subject to certain export restrictions. The current list of countries subject to export restrictions can be found at:

https://swisssign.com/en/support/exportbeschraenkungen

SwissSign reserves the right to request additional documents from the End User in connection with his/her place of residence, as appropriate.

If you have any questions or concerns in this regard, please do not hesitate to contact SwissSign.

4. Duties to cooperate

During the registration process, the End User must provide true and complete information to SwissSign or the identification authorities appointed by SwissSign. He must refrain from granting third parties access to his means of authentication for the user account, particularly his registered smartphone. Records of your personal password may not be disclosed to any other person, must be stored securely and separately from your mobile phone and protected from access by third parties. Access data, such as your password, must be selected in such a way that they cannot be guessed by third parties. In particular, access data may not contain any information about the End User, e.g. first name, last name or date of birth.

The End User shall ensure that no signatures are created if he suspects that his personal password or other access data which must be provided in the authentication process in order to trigger the signature has been stolen or become known to a third party. In the event of loss of the smartphone, the End User must inform SwissSign immediately. As soon as there are changes to the End User's mobile phone number or identity data, SwissSign or the registration authority appointed by SwissSign must be notified and, if necessary, a new identification must be activated. The End User must ensure that his registration with the signature service, including the changed identity data, is up to date.

The End User must utilise all current options to protect his smartphone against attacks by viruses and other malware (e.g. worms or trojans) and must use up-to-date software from a trustworthy source for this purpose.

Any discrepancies in the digital certificate must be reported to SwissSign or the Registration Authority immediately.

5. Legal effect

SwissSign's Sign Service can create a qualified electronic signature pursuant to Article 2(e) ESigA and a simple electronic signature pursuant to Art. 2(a) ESigA and in accordance with the applicable Policies.

You can find the current Policies at the following link:

https://www.swisssign.com/en/support/repository

The type of signature required in the relevant legal transaction is determined by law and, additionally, by other requirements or by the business customer's application using the SwissID Sign Service and is beyond the control of SwissSign.

Under Swiss law, only a qualified electronic signature pursuant to ESigA that is associated with a qualified timestamp is deemed equivalent to a handwritten signature.

The End User is aware that the electronic signatures made with the Sign Service may have different effects if the law of a country other than Switzerland applies and that any existing formal requirements may not be met.

6. Usage period

6.1 Usage for qualified electronic signatures

The End User can use the Signing Service for as long as the certificate issued is valid. The validity period of the certificates is limited to the duration indicated in the certificate. The usage period for the Signing Service may be extended as long as the last identification is no more than five (5) years old, and the End User applies for a new certificate.

The End User shall be solely responsible for ensuring that the identification process is conducted again within five years so that valid certificates are continuously available to him.

The End User undertakes to cease using certificates that have been declared invalid or that have become invalid following expiry of the time limit.

6.2 Usage for simple electronic signatures

The End User can use the Signing Service under the fee-based right of use and subject to the contractual agreements (see sec. 7).

7. Fee-based right of use

The End Customer acquires the right to use a maximum number of signatures (packet) for utilising the SwissID Sign solution (https://www.swissid.ch/en/sign). This right may be exercised for a validity period of 24 months from the date of purchase of a packet. **If the right to use the signatures is not exercised in full within 24 months, it shall be forfeited without replacement or compensation. Packets cannot be accumulated.**

The applicable prices and maximum number of signatures per packet shall be published on the website https://www.swissid.ch/en/sign.

8. Handling of End User data

8.1 Collected data

In the course of providing the services, SwissSign shall only collect, store and process data that is necessary for using the signature service. The handling of this data is governed by the applicable Swiss laws (in particular: Swiss Federal Act on Data Protection (FADP, SR 235.1) and ESigA) also in accordance with the relevant Policies.

For the purpose of creating the digital certificate and maintaining verifiability, SwissSign collects and stores in particular the following data from you:

- Copy of the relevant pages of the identity document presented by you (passport, identity card), including the attributes contained therein
- Images of the face of the End User, if he or she is using online identification tools

- If available: other documents introduced by the End User, including the information contained therein
- Personal means of authentication used
- Log files on any signing processes
- Data concerning the revocation of the certificate
- Other information provided by the End User in the identification process, e.g., his e-mail address

The management and the duration of the storage of such data shall be in accordance with the statutory provisions.

8.2 Digital certificate for qualified electronic signature

Based on the data which has been provided by you and collected in the identity verification process, SwissSign shall, at the request of the subscriber application and upon the End User's stated consent, issue a qualified certificate, which may contain the following information concerning you:

- First name(s), last name
- Two-digit ISO 3166 country code (nationality or residence)
- Information to ensure the uniqueness of the digital certificate

The digital certificate is included in the electronically signed file after completion of the signing process. Anyone in possession of the digitally signed file may view the aforementioned information from the digital certificate at any time. This enables third parties to verify your personal information and to see that the information was registered with SwissSign as a Swiss certification service provider and that the certificate and the signature were issued by SwissSign.

8.3 Simple electronic signature

Based on the data that you provide and SwissSign collects during the SwissID registration process, SwissSign issues a signature containing the following information:

- Given name(s), surname
- Email adddress

Following completion of the signing process, the digital signature is contained in the electronically signed file. Anyone in possession of the digitally signed file may view the aforementioned information from the digital signature at any time.

8.4 Audit trail report

In the case of the simple electronic signature with SwissID Sign, SwissSign also makes an “audit trail report” available if this has been contractually agreed.

This report is made available in PDF format to all persons involved in the signature process and it can be downloaded.

The report contains the following data:

- Email address
- IP address of the device
- Device information (operating system type and version)
- Mobile phone device type
- List of activities, including time
- Name of the signed document
- Hash of the signed document
- Technical, non-personal data

The management and the duration of the storage of such data shall be in accordance with the statutory provisions.

8.5 Data archiving after completion of the signing process

SwissSign complies with the applicable statutory provisions when storing various data relating to the identity verification process, the digital certificate issued for the End User and the signing process. The data is stored for 11 years. The relevant date for the retention period is the date on which the underlying certificates become invalid. This ensures that the digitally signed document can still be verified as correct in the years after it is created. SwissSign records all relevant information concerning the data issued and received by SwissSign and keeps it in safekeeping so that it is available, for the purposes of enabling corresponding evidence to be provided in judicial proceedings, in particular, and ensuring continuity of the service.

SwissSign stores the following data in particular:

- Log files for the signing process
- Hash value of the signed document
- Data concerning the revocation of the certificate
- Data as mentioned in chapter 8.1

9. Fulfilment of duties by SwissSign

SwissSign may engage third parties in order to fulfil its duties, particularly as regards the implementation of the identity verification process by external registration authorities and the retention of identity verification documentation. The End User agrees that the data and information required for this purpose may be disclosed to third parties.

10. Liability

SwissSign shall be liable to the End User for all damages it causes unless it can prove that it is not at fault. Liability for ordinary negligence is excluded.

SwissSign shall be liable for any fault in respect of personal injury.

SwissSign is liable for the conduct of its auxiliaries and any third parties involved (e.g. subcontractors and suppliers) in the same manner as for its own.

In terms of qualified electronic signatures, liability shall also be governed by the relevant provisions of the ESigA. Any further liability is excluded to the extent permitted by law. In particular, the following exclusions apply:

Liability for the proper functioning of third-party systems, particularly liability for hardware and software utilised by the End User or for business customers using the Signing Service applications, is excluded.

SwissSign shall not be liable to you for loss or damage incurred by you due to the fact that you have either failed to comply with or have exceeded a limitation of use.

SwissSign shall bear no liability for the validity of transactions concluded with the aid of certificates.

SwissSign's liability for indirect losses, consequential losses, data loss, data accuracy, third-party losses and lost

revenues and profits, as well as for all financial losses, is excluded to the extent permitted by law.

Furthermore, SwissSign shall not be liable if, because of force majeure, the performance of the service is occasionally interrupted, restricted in whole or in part, or rendered impossible.

The term “force majeure” includes in particular natural phenomena of particular intensity (avalanches, flooding, landslides, etc.), acts of war, riots, and unforeseeable official restrictions (e.g. because of pandemics).

11. Issuance and invalidation of certificates

The End User may at any time request the invalidation of a certificate used by him. This can be done, for example, via an online application in the user account at https://www.swissid.ch/en/ by providing the blocking password or by using the still-valid signature certificate.

SwissSign is entitled to refuse to issue certificates without stating reasons.

SwissSign is authorised to declare certificates invalid on its own initiative. This applies in particular if:

- the certificates were obtained unlawfully or the information provided at the time the application was made is not accurate;
- there is no longer any guarantee that the certificates can only be attributed to the certificate holder (e.g. because the algorithms underlying the signature certificate have been broken);
- the contractual relationship is terminated;
- the End User breaches a duty of cooperation within the meaning of Section 4.

If the invalidation is due to a circumstance attributable to the End User, SwissSign is entitled to compensation for inconvenience and expenses. The right to assert additional damages is expressly reserved.

12. Amendments to the Agreement

SwissSign may adjust or amend the products/services and these Terms and Conditions of Use at any time. This shall be communicated to the End User in an appropriate manner. If the End User disagrees with a material change that is detrimental to him, he shall be entitled to terminate the Agreement in writing within 30 days of notification of the contractual change. If the End User does not object to the changes on time, they shall be deemed to have been accepted.

13. Warranty

The Customer must inspect the certificates and the material provided by SwissSign upon receipt and immediately notify SwissSign in writing of any defects, incorrect and/or incomplete information prior to the first use. Defects discovered later must be reported immediately upon discovery; otherwise, the rights as to defects shall be deemed to have lapsed.

In the event that a defect is reported, SwissSign shall be entitled to choose between rectification and replacement. Any further rights as to defects are expressly excluded. Defective certificates shall be declared invalid by SwissSign.

14. Term / termination of the Agreement

Unless otherwise provided by contract, the Agreement on qualified electronic signature is concluded for an indefinite term.

The Agreement may be terminated by either party with one week’s notice to the end of a month.

If the Customer is not responsible for the reasons for termination, SwissSign shall reimburse the Customer on a pro rata basis for the remuneration paid. Certificates affected by the termination of the Agreement shall be declared invalid by SwissSign.

In the case of simple electronic signature, the term of the Agreement and the rules on termination are governed by the underlying contract.

15. Applicable law and jurisdiction

All legal relationships in connection with these Terms and Conditions of Use shall be governed exclusively by Swiss law and the United Nations Convention on Contracts for the International Sale of Goods of 11 April 1980 shall not apply.

The exclusive place of jurisdiction is Zurich. Mandatory places of jurisdiction remain reserved.

16. Contacts

In case of complaints and/or other general requests as questions regarding the provision of services in accordance with these Terms and Conditions of Use, you may contact SwissSign at the following address: support@swissid.ch.

17. Final provisions

The Customer may not offset claims of SwissSign with any counterclaims.

The Customer may not transfer the rights and obligations under this Agreement to any third party.

All intellectual property rights over the material provided by SwissSign (documentation, devices, software, etc.) shall remain the property of SwissSign or the third parties with rights thereto. The Customer shall receive a non-exclusive and temporally limited licence to use such material in line with the contractual purpose.

If individual provisions of these Terms and Conditions of Use are found to be invalid or unlawful, this shall not affect the validity of the remaining provisions thereof. In such cases, the invalid provision shall be replaced with a valid provision that is as consistent as possible with it in economic terms.

SwissSign AG
Sägereistrasse 25
8152 Glattbrugg
Switzerland
https://www.swissid.ch

March 2025