SwissSign

Terms and Conditions of Use of "SwissSign Signature Service" for eIDAS qualified electronic signature and advanced electronic signature

1. Applicability

These Terms and Conditions of Use shall apply in the relationship between the End User and SwissSign GmbH, Fleischmarkt 1/6/12, 1010 Vienna, Austria (hereafter: "SwissSign") in connection with the use of the SwissSign Signature Services and the corresponding certification services for the electronic signature (hereafter: "Signature Service").

The Terms and Conditions of Use shall be displayed to the End User at the time of the electronic order for the Signature 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.

2. Compliance with regulatory requirements

Insofar as the Signature Service is subject to statutory requirements, SwissSign warrants compliance with the relevant requirements of EU Regulation 910/2014 (eIDAS), the Austrian signature law and the applicable ETSI standards. SwissSign shall in this regard be subject to independent oversight by the competent bodies (Austrian supervisory body - RTR) and regular audits according to the relevant standards by an accredited assessment body.

3. Service

SwissSign offers the End User the option of signing documents using an electronic signature, which may be either a qualified electronic signature or an advanced electronic signature.

3.1 Qualified electronic signature and advanced electronic signatures

The services in connection with qualified electronic signatures under EU Regulation 910/2014 (eIDAS) shall be provided in accordance with the relevant applicable Certificate Policies. These form an integral part of these Terms and Conditions of Use.

The CP/CPS/CPR may be obtained in their most up-to-date form at https://www.swisssign.com/en/support/repository. Specifically, the Relying Party Agreement (RPA) is available at https://repository.swisssign.com/RelyingPartyAgreement.pdf

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

SwissSign shall issue a signature certificate containing information on an identified person. The certificate makes it possible to affix qualified and advanced electronic signatures to documents only 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.

3.1.1 Identification of signatories

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

For the issuance of certificates and the associated qualified electronic signature or advanced electronic signature, the identity of the End User is verified either through a face-to-face meeting or via a remote identification process, using a passport or an identity card recognized in Austria. The authenticity of the identity document is also verified.

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.

3.1.2 Signature creation

Provided all requirements are met, SwissSign creates a personal certificate and the corresponding private cryptographic key on the Hardware Security Module (HSM) managed by the SSASC for the purpose of creating the signature. The supported signature format is PAdES. The signature parameters can be consulted in section 2.4 of the CPR document.

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.

3.1.3 Verification of the qualified electronic signature's validity

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

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

Please note, when verifying the signature with RTR and/or Adobe Acrobat, the respective Terms and Conditions of RTR and/or Adobe Acrobat apply to this verification and SwissSign cannot assume any liability in this regard.

3.2 System availability

SwissSign endeavours to ensure that the Signature Service operates as continuously as possible. SwissSign assumes no liability for the continuous availability of the Signature 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.

The certificate status services provide information on the status of certificates at all times, even after the certificate has expired or was revoked. The response times of the certificate status services can be consulted in section 4.10 of the CPS.

In case of CA key's compromise, SwissSign will schedule the revocation of the affected certificates as described in the Business Continuity Management plan.

In case of termination, SwissSign will transfer obligations for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period such as registration information, certificate status information, and event log archives that cover the respective time to the appropriate organization.

4. Requirements for using the service

The End User is aware of the use and legal consequences of electronic signature certificates pursuant to eIDAS. He must have access to an internet portal or business application that uses the Signature Service provided by SwissSign. He must also have an identity at the necessary security level for using the Signature Service. In addition, for the use of qualified electronic signatures or advanced

electronic signatures, a smartphone with iOS 17.6 or later or Android 9.0 or later (including fingerprint scanner / facial identifier and secure element) is required for triggering the signing process. Additional provisions that may restrict the use of the Signature Service are set out in the terms and conditions of the business customer's applications that use the Signature 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.

4.1 SwissSign obligations

The following obligations are applicable for SwissSign as the provider of the certificate used in the Signature Service,

SwissSign must communicate changes to the CPS and these terms and conditions in accordance with the provisions of the CPS.

SwissSign must issue certificates that are in accordance with the information known at the time of issue, and free of data entry errors.

SwissSign must revoke certificates under the terms set out in the CPS .

SwissSign must make the certificates corresponding to the CA available to applicants.

SwissSign must protect the CA's private key.

SwissSign must use reliable systems and products that are protected against any alteration and that guarantee the technical and cryptographic security of the certification processes they support.

SwissSign must operate in accordance with the applicable legislation.

SwissSign must maintain an updated repository of certificates, indicating the certificates issued and whether they are still valid, revoked or have expired.

4.2 Subscriber obligations

The End User is aware of the use and legal consequences of electronic signature certificates pursuant to eIDAS. The following obligations are applicable for the subscriber of the certificate used in the Signature Service:

The subscriber must provide SwissSign and/or the Registration Authorities with accurate, complete, and truthful information in relation to the data requested by them in order to carry out the process of issuance or termination of the certificate used in the eIDAS Signing Service.

The subscriber must notify any modification of the data supplied in the registration process or any modification of the circumstances reflected in the electronic certificate used in the Signature Service.

The subscriber must know and accept the Terms and Conditions of Use of the electronic certificates used in the eIDAS Signing Service.

The subscriber must use the electronic certificate used in the Signature Service and its keys correctly and not use the signature creation data or private key when the validity period of the electronic certificate has expired.

The subscriber must communicate to SwissSign through the mechanisms provided for this purpose, any malfunction of the electronic certificate used in the eIDAS Signing Service.

The subscriber must protect their signature activation data and authentication mechanisms, taking reasonable precautions to prevent their loss, disclosure or unauthorized use.

The subscriber must comply with the obligations and assumptions that are established for the user in the CPS.

5. 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, particularly his registered smartphone. Records of End User's personal password may not be disclosed to any other person, must be stored securely and separately from End User's mobile phone and protected from access by third parties. Access data, such as End User's 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/she 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 immediately.

6. Legal effect

SwissSign's Signature Service can create a qualified electronic signature pursuant to Art. 3 No. 12 eIDAS and an advanced electronic signature pursuant to Art. 3 No. 11 eIDAS 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 SwissSign Signature Service and is beyond the control of SwissSign. Under eIDAS, only a qualified electronic signature is deemed equivalent to a handwritten signature.

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

7. Usage period

7.1 Usage for qualified electronic signatures and advanced electronic signatures

The End User can use the Signature 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 Signature Service may

be extended as long as the identity document provided is valid, all provided identity information is correct, 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 a corresponding request is received by SwissSign in a timely manner so that any registration process can be carried out and 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.

8. Fee-based right of use

The End User acquires the right to use a maximum number of signatures (packet). 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.swisssign.com/en/digital-signatures.html.

9. Handling of End User data

9.1 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 Austrian laws, GDPR, eIDAS and 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 the End User:

- 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
- Other information provided by the End User in the identification process, e.g., his e-mail address

9.2 Digital certificate for qualified electronic signature and advanced 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 the End User:

- First name(s), last name or pseudonym
- 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 allows third parties to verify the subjet's personal information and confirm that such information has been registered with SwissSign as a trust service provider. It also enables verification that the certificate and associated digital signature were issued by SwissSign.

9.3 Data archiving after completion of the signing process

In order to ensure compliance with statutory requirements for all eIDAS services, as the certification and registration authority, SwissSign must retain all certificate holder data, documentation, audit information and signing process information for a period of 30 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 as mentioned in chapter 9.1

10. 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.

11. 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.

Liability shall also be governed by the relevant provisions of eIDAS. 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 eIDAS 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 of SwissSign.

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).

12. 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 5.

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.

13. 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.

14. 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.

15. Term / termination of the Agreement

Unless otherwise provided by contract, the Agreement on qualified and/or advanced electronic signatures 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.

16. Applicable law and jurisdiction

All legal relationships in connection with these Terms and Conditions of Use shall be governed exclusively by Austrian 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 Vienna, Austria. Mandatory places of jurisdiction remain reserved.

17. Out of court dispute resolution

The Parties shall endeavour to resolve disputes amicably before applying to the ordinary courts and undertake to participate in out of court dispute resolution procedures prescribed by law, to the extent of their statutory duties.

18. Contacts

If you have any questions regarding the provision of services in accordance with these Terms and Conditions of Use, you may contact SwissSign at the following address: https://www.swisssign.com/en/support/kontakt.html.

19. 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 license 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 GmbH
Fleischmarkt 1/6/12
1010 Vienna, Austria
https://www.swisssign.com/en/digital-signatures.html

August 2025