SwissSign

Subscriber Agreement for "SwissSign Signature Service" for eIDAS qualified electronic signature and advanced electronic signature

1. Parties

This Subscriber Agreement (hereafter: "Agreement") governs the Signature Service for eIDAS qualified electronic signature and advanced electronic signature (hereafter: "Signature Service") provided by SwissSign GmbH, located at Fleischmarkt 1/6/12, 1010 Vienna, Austria (hereafter: "SwissSign"), and is entered into between:

- SwissSign GmbH, a qualified trust service provider (QTSP) under Regulation (EU) 910/2014 (eIDAS) and its amendment Regulation (EU) 2024/1183 (eIDAS 2.0).
- Subscriber: the individual that subscribes to and uses the SwissSign Signature Service for eIDAS. The Subscriber is responsible for the proper use, security, and management of their electronic signature in compliance with the terms of this Agreement and relevant legal requirements.

2. Purpose and scope

This Agreement establishes the rights, obligations, and responsibilities of the Subscriber and the SwissSign regarding the issuance, use, and management of a Qualified Electronic Signature (QES) or an Advanced Electronic Signature (AES) certificate issued by the QTSP to the Subscriber.

3. Definitions

- QES (Qualified Electronic Signature): An electronic signature that meets the requirements of eIDAS qualified electronic signature, using a qualified certificate issued by a QTSP.
- AES (Advanced Electronic Signature): An electronic signature that meets the requirements of eIDAS advanced electronic signature, using a qualified certificate issued by a QTSP.
- Private Key: The cryptographic key under the sole control of the Subscriber used to create a QES
- Qualified Certificate: A digital certificate issued by the QTSP verifying the identity of the Subscriber for the purpose of AES and QES.

4. Agreement|

The "Terms and Conditions of Use of SwissSign Signature Service for eIDAS qualified electronic signature and advanced electronic signature" available under Signature Service Terms and Conditions of Use are an integral part of this Agreement as well as all procedural policies associated with this service which are available under https://www.swisssign.com/en/support/repository

5. Requirements for using the service

The Subscriber needs access to an internet portal or business application that uses the signature service provided by SwissSign.

The Subscriber needs an identity at the necessary security level for using the Signature Service.

For the use of QES or AES the Subscriber needs a smartphone with iOS 17.6 or later or Android 11.0 or later (including fingerprint scanner/facial identifier and secure element) to complete the signing process.

6. Subscriber eligibility and verification

The Subscriber confirms to be legally authorized to enter this Agreement.

Subscriber identity must be verified by SwissSign or a registration authority appointed by the QTSP through one of the following mechanisms:

- In-person verification
- Video identification

During the registration process, the Subscriber must provide true and complete information to SwissSign, or the identification authorities appointed by the QTSP.

Qualified 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.

7. Subscriber obligations

The Subscriber is aware of the use and legal consequences of electronic signature certificates pursuant to eIDAS. The following obligations are applicable to 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 Signature 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 SwissSign Signature Service for eIDAS qualified electronic signature and advanced electronic signature".

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 Signature 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 use the Signature Service only for lawful purposes consistent with this Agreement.

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

The Subscriber is particularly aware that the Signature Service is subject to certain export restrictions. The current list of countries subject to export restrictions can be found at:

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

The Subscriber is aware that the electronic signatures made with the Signature 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.

The usage of the QES, AES and the certificate is limited to the certificate's validity period as shown on the certificate.

8. SwissSign obligations

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

SwissSign must communicate changes to the CPS and these Agreement 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.

9. Certificate validity

The QES and AES certificates are valid only while the private key is under exclusive control and the certificate has not been revoked or suspended by the QTSP.

The Subscriber is responsible for ensuring the validity conditions are maintained.

The Subscriber can validate a certificate on the website of Austrian supervisory body - RTR or directly in Adobe Acrobat.

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.

10. Liability and limitations

SwissSign shall be liable to the Subscriber 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 as applicable. 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 Subscriber or for business customers using the Signature Service applications, is excluded.

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

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

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 Signature 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).

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

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

11. Termination

This Agreement may be terminated by the Subscriber or SwissSign with one week prior written notice before the end of the month.

Termination automatically triggers revocation of the Subscriber's QES and AES certificates.

Upon termination, the Subscriber shall no longer use the QES and AES certificates and must securely delete or disable access to the Private Key if feasible.

If the Subscriber is not responsible for the reasons for termination, SwissSign shall reimburse the Customer on a pro rata basis for the remuneration paid.

12. Data protection

Personal data will be processed according to GDPR (EU) or applicable local data protection laws.

Subscriber consent is obtained for the processing of personal information for QES and AES certificate issuance, revocation, and verification purposes.

SwissSign ensures confidentiality and integrity of the data during all operations.

In order to ensure compliance with statutory requirements for all Signature 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.

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 Subscriber agrees that the data and information required for this purpose may be disclosed to third parties.

13. Contacts

In case of complaints, in the event of loss of the smartphone or loss of sole control to the Subscriber's means of authentication and/or other general request as questions regarding the provision of services in accordance with these Agreement, the Subscriber may contact SwissSign at the following address:

https://www.swisssign.com/en/support/kontakt.html.

14. Amendments

SwissSign may adjust or amend the products/services and this Agreement at any time. This shall be communicated to the Subscriber in an appropriate manner.

If the Subscriber disagrees with a material change that is detrimental to them, they shall have the right to terminate the Agreement in writing within 30 days of receiving notice of such change. If the Subscriber does not object to the changes on time, they shall be deemed to have been

accepted.

15. Applicable law and jurisdiction

All legal relationships in connection with these Agreement 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.

Any disputes arising from this Agreement shall be resolved exclusively through the competent courts in Vienna, Austria.

16. Miscellaneous

If any clause is found invalid, the remainder of the Agreement remains enforceable.