SwissSign

SwissSign PDS Certificate Services

PKI Disclosure Statement for Certificate Services

Document Type:	PKI Disclosure Statement
OID:	n/a
Author:	Product Management
Applicability:	Global
Owner:	CEO
Issue Date:	16 February 2024
Version:	4.0
Obsoletes:	3.0 (06.04.2022)
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

Disclaimer: The electronic version of this document and all its stipulations are considered binding and may not be altered by any side agreements.

SwissSign

Version Control

Date	Version	Comment	Author
14.07.2017	1.0	Creation	Ingolf Rauh
14.07.2021	2.0	New chapter 3.8, Several minor changes	Adrian Mueller
06.04.2022	3.0	Deletion chapter 3.6 (SuisseID), update product names & validation QES certificates, minor changes	Adrian Mueller
16.02.2024	4.0	Add eIDAS changes	Luis Peñalosa

SwissSign

Table of Contents

1. Scope

In applying for certificates and services that are based on one of the root certificates publicly provided by SwissSign, the Subscriber to a certificate service (hereafter SUBSCRIBER) consents to the Subscriber Agreement (hereafter SUBSCRIBER AGREEMENT). A SUBSCRIBER means an applicant for a SwissSign certificate, which acquires it from SwissSign and issues it in its own right or for another party [a subject] (server or other person, hereafter CERTIFICATE HOLDER). A SUBSCRIBER may also refer to the recipient of a time stamp and/or a signature. It may be an organisation or an individual end user.

The SUBSCRIBER AGREEMENT shall govern the contractual relationship between the SUBSCRIBER and SwissSign AG, Sägereistrasse 25, 8152 Glattbrugg, Switzerland (hereafter SWISSSIGN) concerning the usage of SWISSSIGN certificates (hereafter referred to collectively as CERTIFICATE SERVICES).

For the eIDAS trust services the SUBSCRIBER AGREEMENT shall govern the contractual relationship between the SUBSCRIBER and SwissSign GmbH,Fleischmarkt 1, Vienna, Austria (hereafter SWISSSIGN) concerning the usage of SWISSSIGN certificates (hereafter referred to collectively as CERTIFICATE SERVICES). A SUBSCRIBER may acquire certificate services either directly or through a Specialist Retailer. The SUBSCRIBER or a third party designated by the SUBSCRIBER or a device may be regarded as the certificate holder (subject) for the certificates concerned, hereafter CERTIFICATE HOLDER. Certificates shall be issued in accordance with the provisions of the following documents: Trust Service Practice Statement (TSPS), Certificate Policy (CP) and Certificate Practice Statement (CPS) for the CA of the relevant root certificate. These policy documents may be obtained in their most up-to-date form at https://repository.swisssign.com.

Compliance with the commercial contractual terms and conditions, which are the basis for usage by the SUBSCRIBER, is a prerequisite for the usage of the CERTIFICATE SERVICES. The commercial contractual terms and conditions are not an integral part of this SUBSCRIBER AGREEMENT. They may also be agreed to between third parties (e.g. Specialist Retailer, employer of the Subscriber etc.).

For contractual purposes, the SUBSCRIBER AGREEMENT and any commercial contractual terms and conditions shall continue to apply, as shall the relevant TSPS, CP and CPS for the issuing of certificates. The PKI Disclosure Agreement shall not replace this and only contains a summary for information purposes of the key points of these two documents in order to facilitate understanding by SUBSCRIBERS, CERTIFICATE HOLDERS and third parties (RELYING PARTIES).

2. CA Contact Info

SwissSign AG:
Postal address: Sägereistrasse 25, 8152 Glattbrugg, Switzerland.
Telephone: ++41 800 55 77 77
Email: helpdesk@swisssign.com

For eIDAS trust services:

SwissSign GmbH:
Postal address: Fleischmarkt 1, Vienna, Austria
Telephone: +41 800 55 77 77
Email: helpdesk@swisssign.com

3. Certificate type, validation process and usage

3.1 Personal S/MIME E-Mail ID Silver

Intended usage:
With the Personal S/MIME E-Mail ID Silver certificate you can reliably sign and encrypt your emails with all common email programs and mail gateways. The software-based certificate contains the validated email address.
Period of validity of 1, 2 or 3 years, software-based, i.e. certificate file. Different validity periods may be set specifically for individual projects.

Validation process:
Only the existence and access of the SUBSCRIBER to the email address is checked. Issuance may be blocked for email addresses in relation to which there is a suspicion of abuse.
If any further attributes are contained in the subject line of the certificate, these will be examined as described under Pro S/MIME E-Mail Gold ID.

Limitations:
This certificate cannot be used for advanced or qualified signatures under Swiss or EU law. In addition, no authorisation is possible.

3.2 Pro S/MIME E-Mail ID Gold

Intended usage:
With the Pro S/MIME E-Mail ID Gold certificate, you can reliably sign and encrypt your emails with all common email programs and mail gateways. You can also use it for authentication purposes (login). The software-based certificate shall contain the validated email address, the applicant's verified

data and, if the organisation entry option has been selected, the verified data of the organisation. A pseudonym may also be provided instead of the applicant's name. The software-based certificate shall be issued for periods of 1 year, 2 years and 3 years. Different validity periods may be set specifically for individual projects.

Validation process:
The CERTIFICATE HOLDER shall be examined by the Registration Authority in person or by presentation of a copy of an official identification document and validation of the signature on the application for the certificate. Within the Managed PKI environment, the examination may also be performed by a Corporate Registration Authority, which e.g. examines the employment contract or obtains the approval of the line manager of the individual concerned or carries out equivalent examinations compared to a face to face check of the CERTIFICATE HOLDER. Any organisation mentioned in the certificate shall be subject to the SwissSign rules on the examination of organisations, which validate its existence with reference to entries in the Commercial Registry, expert reports or similar secure methods.

Limitations:
This certificate cannot be used for qualified signatures. In addition, it cannot be used for advanced signatures that are based on a qualified certificate.

3.3 DV SSL Silver

Intended usage:
The SwissSign DV SSL Silver certificate offers authentication and protection for encrypted communication with devices and websites (DV: Domain Validation). The DV SSL Silver certificate, which is issued within seconds, is the right choice wherever encrypted and cost-effective digital communication is required.

If the DV SSL Silver certificate is only ordered with one domain entry, protection for the domains is included with and without 'www'. The organisation and business activity of the certificate holder is not checked. The certificate is also offered as a wild card (any direct sub-domains). The certificate only contains validated domain names and may be obtained as a 1-year certificate. Different validity periods may be set specifically for individual projects. The certificate is software-based.

Validation process:
The SUBSCRIBER must demonstrate access to the domain address to be protected. Any domain addresses in relation to which there is a suspicion of abuse may be refused. The examination complies with the requirements of the CA Browser Forum.

Limitations:
This certificate cannot be used as a qualified website certificate pursuant to EU Regulation 910/2014 (eIDAS).

3.4 OV SSL Gold

Intended usage:
With the OV SSL Gold certificate validated on organisation level your customers and partners can be certain that your website or your website applications are your own (OV: Organizational Validation). This is because the website operator verified by us is indicated transparently in the certificate. OV SSL Gold offers effective protection, enhanced security and a high level of trust in your company. The OV SSL Gold certificate can also be operated as a multi-domain certificate with further domain entries or as a wild card certificate for any number of sub-domains. It is issued as a software-based certificate for periods of 1 year. Other (shorter) periods may be set specifically for individual projects.

Validation process:
The SUBSCRIBER must demonstrate access to the domain address to be protected. Any domain addresses in relation to which there is a suspicion of abuse may be refused. The organisation indicated in the certificate shall also be verified with reference to registers and the consent provided by authorised signatories. The examination complies with the requirements of the CA Browser Forum.

Limitations:
This certificate cannot be used as a qualified website certificate pursuant to EU Regulation 910/2014 (eIDAS).

3.5 EV SSL Gold

Intended usage:
With the EV SSL Gold certificate you can achieve the highest level of trust with visitors to your website or your web applications (EV: Extended Validation). The EV SSL Gold certificate offers optimal protection and security for your clients and business partners. The EV SSL Gold certificate can also be operated as a multi-domain certificate with further domain entries. It is issued as a software-based certificate for a period of 1 year. Other (shorter) periods may be set specifically for individual projects. Alongside domain names, organisation names and organisation addresses, the certificate also contains official registry information relating to the organisation.

Validation process:
The SUBSCRIBER must demonstrate access to the domain address to be protected. Any domain addresses in relation to which there is a suspicion of abuse may be refused. The organisation indicated in the certificate shall also be verified with reference to registers and the consent provided by

authorised signatories. It is subject to particularly stringent examinations by the CA Browser Forum for EV certificates, which also includes an examination of business operations.

Limitations:
This certificate cannot be used as a qualified website certificate pursuant to EU Regulation 910/2014 (eIDAS).

3.6 Regulated seal certificate

Please note: This product is end of sale.

Intended usage:
The regulated seal certificate is a regulated certificate (according to ZertES) for an organisation. It is permitted for special signatures defined in the relevant legislation. It is i hardware-based and is issued for periods of one and three years. Other periods may be set specifically for individual projects. Alongside the official registry number and optional address information, the regulated certificate also contains the [name of the] organisation.

Validation process:
The SUBSCRIBER must appear in person before a Registration Authority of SWISSSIGN or visit an identification point stipulated by SWISSSIGN (e.g. Swiss Post "yellow identification" service or a notary public), which will confirm the personal data on his/her ID card and the fact that he/she appeared in person. All information contained in the application shall be controlled with reference to the ID card.

Names of organisations shall be verified with reference to extracts from the Registry and by the signatures of authorised signatories of the organisation.

Limitations:
A regulated seal certificate issued by the Swiss CA cannot be used as a qualified certificate pursuant to EU Regulation 910/2014.

3.7 Personal certificate for the qualified electronic signature (ZertES)

Intended usage:
The personal certificate for the qualified electronic signature (QES) is used to create remote signatures equivalent to the handwritten signature. These certificates meet the requirements of the Swiss Signatures Act (ZertES SR 943.03). The certificates are issued with a validity of 2 years. The qualified certificate contains the name or a pseudonym of the certificate holder. The associated private keys are created and stored on a Qualified Signature Creation Device (QSCD), which fulfils the requirements according to ZertES.

Validation process:
The SUBSCRIBER must appear in person at a SWISSSIGN registration office or at an identification office designated by SWISSSIGN. Alternatively, the SUBSCRIBER can use SWISSSIGN's unattended remote identification process equivalent to the in-person process.
Using an official identification document accepted in Switzerland, the personal data required for the issuance of the certificate will be verified and confirmed.

Limitations:
This certificate cannot be used as a qualified certificate according to the EU Regulation 910/2014 (eIDAS).

3.8 Personal certificate for qualified electronic signature (eIDAS)

Intended usage:
The personal certificate for qualified electronic signature (QES) is used to create remote signatures equivalent to the handwritten signature. These certificates meet the requirements of the Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market also know as eIDAS. The certificates are issued with a validity of 10 minutes. The qualified certificate contains the name of the certificate holder. The associated private keys are created and stored on a Qualified Signature Creation Device (QSCD), which fulfils the requirements according to eIDAS.

Validation process:
The SUBSCRIBER must appear in person at a SWISSSIGN registration office.
Using a Swiss official identification document, the personal data required for the issuance of the certificate will be verified and confirmed.

Limitations:
This certificate cannot be used as a qualified certificate according to the Swiss Signatures Act (ZertES SR 943.03).

3.9 Personal certificate for advanced electronic signature (eIDAS)

Intended usage:
The personal certificate for advanced electronic signature (AES) is used to create remote signatures which uniquely links to the signer. These certificates meet the requirements of the Regulation (EU) No 910/2014 on electronic identification and trust services ofr electronic transactions in the internal market also know as eIDAS. The certificates are issued with a validity of 10 minutes. The qualified certificate contains the name of the certificate holder.

Validation process:
The SUBSCRIBER must appear in person at a SWISSSIGN registration office
Using a Swiss official identification document, the personal data required for the issuance of the certificate will be verified and confirmed.

Limitations:
This certificate cannot be used as a qualified certificate according to the Swiss Signatures Act (ZertES SR 943.03).

3.10 Test certificate

Intended usage:
The test certificate is used in production for test purposes. This certificate can only be issued for certain types indicated above.

Validation process:
As a productive certificate, the test certificate is validated in exactly the same way as all other productive certificates.

Limitations:
This certificate should not be used for operational purposes other than testing. SWISSSIGN refuses any liability for this certificate.

4. Limitations on trust

The usage of the certificate is indicated in the intended purpose specified in section 3. This is apparent from the contents of the certificate (e.g. key usage field) also from the examination rules and requirements for this type of certificate.

All data contained in the activity log (data concerning the certificate lifecycle) will be retained for 11 years.

In the case of the eIDAS trust services all data contained in the activity log will be retained for 30 years.

5. Duties of the SUBSCRIBER

The SUBSCRIBER must ensure compliance with the terms of the SUBSCRIBER AGREEMENTS. These require the SUBSCRIBER in particular to comply with the following duties:

5.1 Accuracy of information

The SUBSCRIBER and CERTIFICATE HOLDER represents and warrants that it will at all times provide SWISSSIGN and/or the Specialist Retailer with correct and complete information, both in the certificate application and otherwise, provided said information is requested in connection with the issuance of certificates. This includes but is not limited to domain names, designations of the name and registered office of the organisation, its authorised signatories and access managers. Where changes arise, the CERTIFICATE HOLDER shall contact the SUBSCRIBER and the SUBSCRIBER shall notify SWISSSIGN of them directly if it is in a direct commercial contractual relationship with SWISSSIGN, and otherwise shall notify SWISSSIGN through the Specialist Retailer in an adjustment to the order.

5.2 Key generation

If the SUBSCRIBER generates the key pair itself, it shall choose an algorithm and key length according to ETSI standard TS 119 312, which shall be deemed to be recognised for the usage of this certificate for the duration of the validity period.

5.3 Protection of private key

The SUBSCRIBER represents and warrants that it has taken all reasonable measures and that the CERTIFICATE HOLDER has exclusive control of the private keys. This includes all measures to keep the key confidential and always protect it appropriately.

5.4 Acceptance of certificate

The SUBSCRIBER undertakes and warrants that it shall review the content of the certificate with the CERTIFICATE HOLDER to check that it is accurate.

5.5 Use of certificate

The SUBSCRIBER shall ensure that it installs SSL server certificates only on servers which are accessible under the designation in the subjectAltName of the certificate. All certificates shall be used only pursuant to the applicable law and only in accordance with the SUBSCRIBER AGREEMENT.

5.6 Duty to report and declaration of invalidity (revocation)

The SUBSCRIBER and the CERTIFICATE HOLDER shall ensure that the certificate is revoked immediately or ask SWISSSIGN to declare the certificate invalid if:

a) any information in the certificate is or becomes invalid or false; or
b) the private key is discovered to have been or suspected of having been compromised, misused or stolen in relation to the public key associated with the certificate.
c) If the private key can no longer be accessed.

5.7 Termination of use of certificate

The SUBSCRIBER and CERTIFICATE HOLDER must immediately cease using the private key if misuse or theft of the

private key has occurred and the certificate has been revoked. If the validity period of the certificate has expired, it may only be used further for decryption.

5.8 Response in the event of misuse

The SUBSCRIBER shall within the specified period carry out all of SWISSSIGN'S instructions issued in relation to the theft of the private key. When issuing its instructions SWISSSIGN shall consider ordinary office hours to the extent possible taking account of the urgency and shall endeavour to provide reasonable explanations for its instructions.

5.9 Revocation in the event of breaches of duty

The SUBSCRIBER and CERTIFICATE HOLDER acknowledges and accepts that SWISSSIGN is authorised to revoke a certificate immediately if the SUBSCRIBER or CERTIFICATE HOLDER contravenes the corresponding TSPS, CPS, and CP or other applicable documents or the contractual obligations, or if SWISSSIGN discovers that the certificate has been used for illegal activities, such as phishing, fraud or the dissemination of malware.

If there are indications that the SUBSCRIBER or CERTIFICATE HOLDER is not adhering to further statutory or contractual obligations, SWISSSIGN shall have the right, after issuing a reminder and setting a reasonable grace period in which to remedy the contravention, to revoke all certificates issued pursuant to this Agreement.

5.10 Managed PKI access certificates

A Managed PKI is a certificate service which enables the SUBSCRIBER to issue certificates without individual approval independently for its domains and (depending on the vetting level) for its organisation. The SUBSCRIBER shall receive access certificates for this purpose.

The SUBSCRIBER warrants that all access certificates issued by SWISSSIGN as part of these Managed PKI contracts shall be used in accordance with the provisions of the applicable SWISSSIGN CP/CPS.

It shall ensure that the access certificates are handled carefully in accordance with the protection regulations for certificates as specified above in this paragraph. It must keep the access certificates and the associated passwords separate from each other. It shall be liable for all loss or damage resulting from the unauthorised, unforeseen or careless use of said certificates.

If the SUBSCRIBER has reason to belief that an unauthorised third party knows the means of access to the Managed PKI or can acquire unauthorised access, it must immediately notify SWISSSIGN of this directly.

PINs and passwords must be kept secret and all data concerning these must be kept locked in a secure location which is not accessible to third parties. If third parties have access to its SWISSSIGN account, the SUBSCRIBER shall be liable for their actions as if they were its own.

The SUBSCRIBER must ensure that the operational IT system for this purpose, which is used for the signature and encryption of data, is checked with due care for viruses and kept up to date in order to prevent software from being used whose purpose is to compromise the signatures or certificates.

5.11 Particular compliance with the duty of care

The SUBSCRIBER accepts that any violation of its duties of care may result in financial loss and/or adverse consequences for SWISSSIGN particularly in relation to publicly trusted certificates, such as e.g. exclusion from root programmes or subjection to sanctions in the event of endorsements/certifications, or adverse regulatory consequences.

5.12 No recognition of non-qualified certificates

The SUBSCRIBER acknowledges that SWISSSIGN Platinum CA and Signature Services CA and related TSPS, CP and CPS also enable certificates that are not recognised as qualified or regulated to be issued.

5.13 Duties in relation to Platinum CA certificates

CERTIFICATE SERVICES provided under the SWISSSIGN Platinum CA and related CP/CPS entail particular duties for the CERTIFICATE HOLDER:

The CERTIFICATE HOLDER of a qualified certificate or seal certificate compliant with ZertES shall use it on a secure signature creation device that complies with the law or in accordance with the signature service having regard to statutory requirements. The SUBSCRIBER shall ensure that cryptographic functions and the private key are only used on these devices.

Upon first request by SwissSign, usage of the appropriate signature creation device shall be demonstrated to SwissSign. The CERTIFICATE HOLDER of a certificate issued under the SWISSSIGN Platinum CA and related CP/CPS on a smart card or HSM undertakes to handle this signature creation device with care (smart card, HSM) in accordance with Section 8 also after expiration of the validity of the certificate contained on it.

This device may not be reused.

SWISSSIGN recommends that a secure signature creation device is used for all other certificates.

The SUBSCRIBER acknowledges that SWISSSIGN Platinum CA and related CP/CPS also enable certificates that are not recognised as qualified or regulated to be issued.

5.14 Duties relating to the importing and exporting of certificates

The SUBSCRIBER and CERTIFICATE HOLDER acknowledges that the exporting or importing and usage of CERTIFICATE SERVICES from, to or in countries subject to sanctions and embargoes is prohibited (cf. https://www.swisssign.com/en/support/exportbeschraenkungen.html).

6. Duties of the RELYING PARTY and examination of the certificate

A RELYING PARTY must comply with the terms of the Relying Party Agreement upon receipt of the certificate. The following aspects must be complied with:

- The certificate upon which the signature is based and all certificates in the certificate chain must not have been revoked. SwissSign shall provide standard services for examining the validity of the certificate, such as CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol). Before a signature is trusted, its validity should be verified by the RELYING PARTY. Links to the CRL and OCSP are part of the certificate. CRLs are valid for a maximum of 10 days, although updated daily. The RELYING PARTY must therefore always refer to the most recent CRL file to review the validity of the certificate.
- If for technical reasons no CRL file or OCSP service is available, the RELYING PARTY must estimate itself how long it is able to rely on the validity of the signature. This shall also take account of the related transactions and the attendant risk. Confidence may not be granted for longer than 10 days.
- The validity of SwissSign certificates shall be limited to the validity period of the certificate less 10 days. The RELYING PARTY must therefore always check whether the certificate is still valid.
- For signed documents it is necessary to ensure that the documents have not been changed since the signature was affixed.
- Standard applications should indicate that the signature is reliable under the circumstances indicated in the last point. In particular, the identity of the certificate holder should be correctly indicated.
- It must ensure that the certificate does not contain transaction limits that would preclude the usage of the certificate in relation to a transaction.
- SwissSign certificates are not intended for usage within highly critical infrastructure. Decisions that could result directly or indirectly in personal injury or significant damage to property should not be taken automatically on the basis of SwissSign certificate signatures. Such situations include but are not limited to: the operation of power stations, weapons systems, flight control systems, etc.
- Responsibility for the risk assessment and usage of the certificate within a particular deployment scenario shall lie with the RELYING PARTY.
- Certificates that are no longer valid must not be used.

7. Limitations on liability

Limitations on liability are set forth in the TSPS, CP and CPS. Liability for certificates from the Silver Root CA is in principle limited to CHF 10,000 and for Gold Root CA to CHF 100,000. All qualified certificates and regulated seal certificates are subject to the statutory liability limit laid down in the ZertES (Swiss qualified certificates) and the eIDAS (EU qualified certificates).

SWISSSIGN shall bear full liability towards the SUBSCRIBER for any losses occasioned by it to the SUBSCRIBER unless SwissSign proves that it was not at fault. Liability for minor negligence is excluded.

The liability provisions of the TSPS, CP and CPS apply to third parties.

Neither party shall be liable for the proper functioning of third party systems, including in particular the internet. SWISSSIGN shall not be liable for the systems and software used by the SUBSCRIBER.

The SUBSCRIBER shall fully indemnify SWISSSIGN from all third party claims resulting from use in breach of contract or unlawful or improper use of the CERTIFICATE SERVICE. In this case the exemption shall include also the obligation to indemnify SWISSSIGN in full against legal defence costs (e.g. procedural costs and legal fees).

Both Parties shall be liable for the conduct of their assistants and any third parties who are involved (such as subcontractors and suppliers) in the same way as for their own conduct.

In the event of personal injury, the Parties shall be liable for any fault. Under no circumstances shall the Parties be liable in particular for indirect or consequential losses, data loss, additional expense or claims by third parties, lost profit or

unrealised savings, or losses resulting from late delivery or service.

The provisions governing liability set forth in the Swiss Federal Act on Electronic Signatures and in Article 59a of the Swiss Code of Obligations shall apply under all circumstances on a priority basis for certificates signed by the Swiss CA.

8. Other applicable documents

The following documents shall be relevant for the SUBSCRIBER and the CERTIFICATE HOLDER along with the RELYING PARTY, the most recently updated version of which may be found at https://repository.swisssign.com:

a) CP, CPS and TSPS: certification guidelines and implementing provisions of SwissSign CA.
b) SUBSCRIBER AGREEMENT: provisions setting out the rights and duties of the SUBSCRIBER and CERTIFICATE HOLDER in relation to a certificate service.
c) Relying Party Agreement: provisions setting out the rights and duties of a RELYING PARTY.

9. Privacy Policy

SWISSSIGN undertakes to comply with the data protection legislation applicable to its relevant CA.

The data contained in the certificate shall be regarded as publicly available data.

The data required to provide the services shall be saved and treated as confidential by SWISSSIGN. The data collected as part of inspection activity, including particular personal data, may only be used for the purpose and to the extent required to perform and implement the CERTIFICATE SERVICE. Usage for other purposes or disclosure to any third parties is strictly prohibited. The above shall not apply to disclosure to authorised instructed third parties (e.g. in the event of a control, external registration activity) or in accordance with official requirements. Authorised instructed third parties shall be subject to data protection rules in the same manner as SWISSSIGN.

The security technology used to protect data shall correspond to the state of the art.

The SUBSCRIBER and CERTIFICATE HOLDER undertakes to comply with the provisions of data protection legislation that is locally applicable to it as well as the data protection provisions of the applicable CP, CPS and other applicable documents.

10. Refund Policy

Certificates that are already valid may be refunded in accordance with the commercial GTCs. The most recently updated version may be downloaded from www.swisssign.com/en/agb-swisssign.html.

11. Applicable law, complaints and dispute resolution

For all complaints please refer to the contact data listed on www.swisssign.com/contact.

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.

APPLICABLE LAW AND JURISDICTION

The legal relationship resulting from the SUBSCRIBER AGREEMENT shall be governed exclusively by Swiss law. The provisions of the UN Convention on Contracts for the International Sale of Goods of April 11, 1980 (Vienna Convention, "CISG") are excluded under all circumstances.

The courts of Zurich, Switzerland shall have exclusive jurisdiction. For Subscribers and Certificate holders with a foreign place of residence or registered office, the place of debt enforcement and exclusive jurisdiction for all civil proceedings shall be Zurich, Switzerland.

In the case of the eIDAS courts of Vienna, Austria shall have exclusive jurisdiction. For Subscribers and Certificate holders with a foreign place of residence or registered office, the place of debt enforcement and exclusive jurisdiction for all civil proceedings shall be Vienna, Austria.

12. TSP and repository licenses, trust marks, and audit

Insofar as the issuance and management of certificates is subject to statutory requirements (e.g. in Switzerland the ZertES or in the EU the eIDAS Regulation), SWISSSIGN warrants compliance with the relevant requirements and implementing provisions. SWISSSIGN shall in this regard be subject to oversight by the competent bodies whilst audits and inspections shall be carried out in accordance with the relevant standards applicable to the certificates in question (e.g. ETSI, CA Browser Forum) and statutory requirements.