

## Subscriber Agreement Certificate Services

Version: 2.0

OID: 2.16.756.1.89.1.0.2.0.2

NB: Insofar as the Subscriber acquires the certificate service directly through its organisation or through a reseller (hereafter Specialist Retailer), its organisation shall be obliged to inform the Subscriber, and as the case may be any Certificate Holder that is not a subscriber, concerning this Subscriber Agreement and to require compliance with the terms hereof.

This document is subject to the SwissSign audit as an accredited certification authority and may not be altered, invalidated or amended by any side agreements.

**Approval and versions**

<b>Author</b>	<b>Date</b>	<b>Version</b>	<b>Comments</b>
Ingolf Rauh	2017-07-14	1.0	Creation
Michael Widmer	2020-06-24	2.0	Update typos and minor corrections on usage

**Approval by**

<b>SwissSign authorised signatory</b>	<b>Digital signature</b>
Michael Günther (CISO) SwissSign AG	
Markus Naef (CEO) SwissSign AG	

**Table of contents**

1. Scope .....	4
2. Compliance with regulatory requirements .....	4
3. Contractual Components.....	4
4. Reissuing and change in attributes.....	4
5. Revocation of certificates.....	4
6. Certificate expiration .....	5
7. Directory service.....	6
8. Customer service, helpdesk, support .....	6
9. Duties of the SUBSCRIBER and CERTIFICATE HOLDER when dealing with certificates .....	6
9.1 Accuracy of information .....	6
9.2 Key generation.....	6
9.3 Protection of private key .....	6
9.4 Acceptance of certificate .....	6
9.5 Use of certificate.....	6
9.6 Duty to report and declaration of invalidity (revocation) .....	6
9.7 Termination of use of certificate .....	7
9.8 Response in the event of misuse.....	7
9.9 Revocation in the event of breaches of duty .....	7
9.10 Managed PKI access certificates.....	7
9.11 OCSP Stapling.....	7
9.12 Particular compliance with the duty of care .....	7
10. Special duties for Platinum certificates .....	8
11. Relevant information from SWISSSIGN .....	8
12. Entry into force, duration and termination, effects of termination in general.....	8
13. Claims and discontinuation of CERTIFICATE SERVICES in the event of payment default.....	8
14. Customer data and data protection .....	9
15. Involvement of third parties.....	9
16. Warranty.....	9
17. Liability.....	9
18. Export and import, international use of certificates .....	10
19. Intellectual property rights.....	10
20. Severability of this Agreement .....	10
21. Amendment of the SUBSCRIBER AGREEMENT CERTIFICATE SERVICES.....	10
22. Assignment and transfer of rights and duties .....	10
23. Out of court dispute resolution .....	11
24. Applicable law and jurisdiction.....	11

## 1. Scope

In applying for certificates and services that are based on one of the publicly trusted root certificates of the Swiss or Liechtenstein SwissSign Platinum CA, SwissSign Gold CA or SwissSign Silver CA, 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 (server or other person, hereafter CERTIFICATE HOLDER).

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

A SUBSCRIBER may acquire certificate services either directly or through a Specialist Retailer.

Certificates shall be issued in accordance with the provisions of the CP/CPS of the relevant root certificate. The CP/CPS may be obtained in their most up-to-date form at <https://www.swissign.com/en/cp-repository>.

This SUBSCRIBER AGREEMENT shall be applicable to all SUBSCRIBERS and CERTIFICATE HOLDERS independently of any group relationship between them and the CA. It shall apply as the 'Subscriber Agreement' and the 'Terms of Use Agreement' in accordance with the CA/Browser Forum Baseline Requirements, the ETSI standards and the corresponding programs of the operator of public "Trusted Root Certificate Stores".

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

The SUBSCRIBER acknowledges that no legal claims against SWISSIGN may arise either under this SUBSCRIBER AGREEMENT or from the usage of the CERTIFICATE SERVICE, unless SWISSIGN contravenes any

liability terms and conditions pursuant to section 17 "Liability".

## 2. Compliance with regulatory requirements

Insofar as the issuance and management of certificates is subject to statutory requirements (e.g. in Switzerland the ZertES and OEID; in Liechtenstein the Signatures Act eIDAS), SWISSIGN warrants compliance with the relevant requirements and implementing provisions. SWISSIGN shall in this regard be subject to oversight by the competent bodies (Switzerland: certification authority; Liechtenstein: Office for Communication) 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.

## 3. Contractual Components

The applicable CP/CPS of the signing, trusted root certificate shall be an integral part of this SUBSCRIBER AGREEMENT Certificate Services and shall take precedence in the event of any discrepancies.

The applicable CP/CPS may be obtained in their most up-to-date form at <https://www.swissign.com/en/cp-repository>.

## 4. Reissuing and change in attributes

Reissuing/rekeying: The repeated issuance of certificates is possible. This may either be done using new self-generated keys or by using the already existing key pair, or using a key pair generated by SWISSIGN. All subject and SAN attributes shall remain unchanged. Reissuing may be offered on a self-service basis (web interface) or may occur on an automated basis through a Managed PKI or through the helpdesk of SWISSIGN.

Any changes to the SAN attribute or subject shall require the certificate to be reissued.

## 5. Revocation of certificates

Certificates that have been revoked may no longer be actively used and shall without exception be published as invalid in so-called revocation lists ("CRL") and the online revocation service ("OCSP").

Where appropriate, SWISSIGN may at any time declare the certificate of a SUBSCRIBER or CERTIFICATE HOLDER to be invalid with immediate effect and

without prior notice on grounds including the following within a maximum of 24 hours after the occurrence of the event was discovered:

- a) The CERTIFICATE HOLDER or SUBSCRIBER requests SWISSIGN in writing to declare its certificate invalid,
- b) The SUBSCRIBER or CERTIFICATE HOLDER commits a breach of the agreed terms and/or applicable laws, regulations and ordinances.
- c) The SUBSCRIBER or CERTIFICATE HOLDER informs SWISSIGN that the original certificate request was unauthorised and not approved or that the approval has been withdrawn.
- d) SWISSIGN obtains information suggesting that the private key of the SUBSCRIBER or CERTIFICATE HOLDER, which corresponds to the public key of the certificate, has been potentially compromised or that the certificate has been otherwise potentially misused.
- e) SWISSIGN becomes aware of the fact that the SUBSCRIBER or CERTIFICATE HOLDER has committed a breach of one or more material obligations under this SUBSCRIBER AGREEMENT.
- f) SWISSIGN becomes aware of circumstances that suggest that the usage of a fully qualified domain name or an IP address for the certificate is no longer legally permitted (e.g. a court of law or arbitral tribunal has revoked the right of a party registering a domain name to use the domain name, a relevant licence or service contract between the party registering a domain name and the applicant for the certificate has been terminated or the registration authority for a domain name has failed to renew the domain name).
- g) SWISSIGN becomes aware of the fact that a wild card certificate has been used in order fraudulently to authenticate misleading subordinate fully qualified domain names.
- h) SWISSIGN becomes aware of a change in the information contained in the certificate.
- i) SWISSIGN becomes aware of the fact that the certificate was not issued in accordance with the CA/Browser Forum Baseline Requirements or the applicable CP/CPS of SWISSIGN or can no longer be valid on the basis of new regulations.
- j) SWISSIGN takes the view that information contained in the certificate is imprecise or misleading.
- k) SWISSIGN discontinues operations for any reason and has not made provision for another certification authority to provide support for declaring the certificate invalid.
- l) The right of SWISSIGN to issue certificates that are compliant with the CA/Browser Forum Baseline Requirements has expired or is revoked or terminated and SWISSIGN has not made provision to maintain the CRL/OCSP directories that are relevant for revocation.
- m) SWISSIGN becomes aware that a private key of a SubCA or Managed PKI was used in order to issue the certificate may have been compromised.
- n) The technical content or format of the certificate represents an unacceptable risk for the providers of application software or third parties (e.g. the CA/Browser Forum is able to establish that an obsolete cryptography/key algorithm or an obsolete key size represents an unacceptable risk and that such certificates should be declared invalid and replaced by certification authorities within a particular period of time).
- o) A private key of the SWISSIGN certification authority within the chain of trust of the certificate has been compromised.

Reference is made to the CP/CPS for any further reasons for a declaration of invalidity.

SWISSIGN shall in addition be entitled to investigate all incidents and, where required, to take action as provided for by law.

The certificate in question shall become invalid after the declaration of invalidity. The CERTIFICATE HOLDER shall bear liability for all losses arising in relation to the usage of a certificate that has been declared invalid. SWISSIGN does not accept any liability for losses of any kind whatsoever arising as a result of such usage. The SUBSCRIBER shall have no entitlement to a free replacement of a certificate that has been declared invalid.

The declaration of invalidity of a certificate is described on the website at <https://www.swissign.com/en/revocation>.

## 6. Certificate expiration

The validity period of a SWISSIGN certificate is limited to the maximum remaining duration of the certificate of the issuing CA less 10 days. It shall be the sole responsibility of the Certificate Holder to ensure the uninterrupted usage of SWISSIGN certificates. For this reason, SWISSIGN recommends to the SUBSCRIBER that it apply for a new certificate at least 30 days prior to the expiration of the certificate or com-

mence the certificate renewal procedure at least 1 day prior to expiration of the certificate.

## **7. Directory service**

SWISSIGN manages a public directory service for the certificates it issues. The SUBSCRIBER's certificates shall be published in the directory service with the SUBSCRIBER's consent. The certificates shall bear the name "SWISSIGN" on them as issuer. This enables people to infer that there is a contractual relationship between SWISSIGN and the SUBSCRIBER or between SWISSIGN and the CERTIFICATE HOLDER.

## **8. Customer service, helpdesk, support**

SWISSIGN operates a customer service unit ("Helpdesk" or "Support"). This may be reached using the contact form at <https://www.swissign.com/en/contact> or by email at [helpdesk@swissign.com](mailto:helpdesk@swissign.com). Any comments and feedback concerning this SUBSCRIBER AGREEMENT may also be submitted in this manner.

## **9. Duties of the SUBSCRIBER and CERTIFICATE HOLDER when dealing with certificates**

### **9.1 Accuracy of information**

The SUBSCRIBER and CERTIFICATE HOLDER represents and warrants that it will at all times provide SWISSIGN 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 SWISSIGN of them directly if it is in a direct commercial contractual relationship with SWISSIGN, and otherwise shall notify SWISSIGN through the Specialist Retailer in an adjustment to the order.

### **9.2 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.

### **9.3 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 protect it appropriately at all times.

### **9.4 Acceptance of certificate**

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

### **9.5 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.

The SUBSCRIBER shall use the key of the certificate only for the purpose for which the certificate is issued.

In the case of key management on behalf of the SUBSCRIBER, it is highly recommended that the subject's key pair is used only for electronic signatures.

### **9.6 Duty to report and declaration of invalidity (revocation)**

The SUBSCRIBER and the CERTIFICATE HOLDER shall ensure that the certificate is revoked immediately or ask SWISSIGN 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.

### **9.7 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. This shall also apply in the event that the SUBSCRIBER or the CERTIFICATE HOLDER becomes aware of the fact that a certificate issued by the CA has been compromised within the certificate chain and is no longer valid. If the validity period of the certificate or a certificate in the certificate chain has expired, it may only be used further for decryption. A certificate that has been revoked can no longer be rendered valid.

### **9.8 Response in the event of misuse**

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

### **9.9 Revocation in the event of breaches of duty**

The SUBSCRIBER and CERTIFICATE HOLDER acknowledges and accepts that SWISSIGN is authorised to revoke a certificate immediately if the SUBSCRIBER or CERTIFICATE HOLDER contravenes the corresponding CP/CPS or this Managed PKI Setup Agreement, or if SWISSIGN 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, SWISSIGN 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.

### **9.10 Managed PKI access certificates**

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

The SUBSCRIBER warrants that all access certificates issued by SWISSIGN in accordance with these Man-

aged PKI contracts shall be used in accordance with the provisions of the applicable SWISSIGN 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 9. In particular, it must keep the access certificates and the associated passwords separate from each other. It shall be liable for all loss or damage resulting in particular from the unauthorised, unforeseen or careless use of said certificates.

If the SUBSCRIBER has grounds for assuming that an unauthorised third party knows the means of access to the Managed PKI or can acquire unauthorised access, it must immediately notify SWISSIGN 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 SWISSIGN account, the SUBSCRIBER shall be liable for their actions as if they were its own.

The SUBSCRIBER must ensure that its IT system deployed 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 the usage of software that has the purpose of compromising the signatures or certificates.

### **9.11 OCSP Stapling**

The SUBSCRIBER must ensure where a web site protected by publicly trusted SSL certificates is actively used and, where SSL EV certificates are used, that OCSP Stapling is implemented on the web server.

### **9.12 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 SWISSIGN 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.



## 10. Special duties for Platinum certificates

CERTIFICATE SERVICES provided under the SWISSIGN Platinum CA and related CP/CPS (see 3) entail particular duties for the CERTIFICATE HOLDER:

The CERTIFICATE HOLDER of a qualified certificate or seal certificate compliant with the eIDAS or ZertES shall use it exclusively 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 request by SWISSIGN, usage of the appropriate signature creation device shall be demonstrated to SWISSIGN. The CERTIFICATE HOLDER of a certificate issued under the SWISSIGN Platinum CA and related CP/CPS (see 3) 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.

Platinum certificates that are designated as OEIDI compatible may only be used in accordance with the provisions of the OEIDI Ordinance SR 641.201.1.

Platinum certificates do not specify any upper limit for transaction values.

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

The SUBSCRIBER acknowledges that SWISSIGN Platinum CA and related CP/CPS (see 3) also enable certificates that are not recognised as qualified or regulated to be issued.

## 11. Relevant information from SWISSIGN

All relevant information relating to misuse, compromise, algorithm changes, system failures etc. shall be reported by SWISSIGN through the system status page

<https://www.swissign.com/en/systemstatus>.

## 12. Entry into force, duration and termination, effects of termination in general

The Contract shall take effect upon the issuance of the certificate and shall apply for the duration thereof. It shall end upon expiry of the certificate in question or upon revocation (withdrawal).

The validity of the certificate shall expire upon termination of the Contract. Time stamps and signatures affixed shall remain valid unless and until the signature certificates have been revoked. Any certificates that are still valid shall be revoked.

Notice of termination must always be given in writing.

## 13. Claims and discontinuation of CERTIFICATE SERVICES in the event of payment default

The SUBSCRIBER may not offset amounts due to SWISSIGN against any counterclaims.

The following provisions shall apply in the event of non-payment by the SPECIALIST RETAILER or SUBSCRIBER in relation to the CERTIFICATE SERVICE:

- a) If the SUBSCRIBER or SPECIALIST RETAILER owes the service fee to SWISSIGN, the obligor shall be deemed to be in default at the time a reminder is issued.
- b) If payment is not made within the grace period, in the event that the CERTIFICATE SERVICE was sold through a SPECIALIST RETAILER, SWISSIGN shall inform the SUBSCRIBER of the Specialist Retailer of the default on the part of the Specialist Retailer.
- c) SWISSIGN shall require the SUBSCRIBER directly to make payment of the outstanding services relating to it before a final payment deadline and shall inform it of the impending discontinuation of service in the event of non-payment.

If payment is not made either by a Specialist Retailer or by the SUBSCRIBER before the final payment deadline, SWISSIGN shall be entitled to block access to the CERTIFICATE SERVICES and revoke the relevant certificates that have not been paid for in full or provide the service on a restricted basis.



#### **14. Customer data and data protection**

SWISSIGN 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 SWISSIGN. The data collected as part of inspection activity, including in 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 SWISSIGN.

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 (see 3).

In order to ensure compliance with statutory requirements, as the certification and registration authority, SWISSIGN must retain all certificate holder data, documentation and audit information for a minimum period of 11 years after expiration of a certificate.

The data protection level in Switzerland has been confirmed by the European Commission as adequate. The requirement for the lawful transmission of data from member states of the European Union to Switzerland, namely that there must be an adequate level of data protection in the location in the third country where the data is received, has consequently been met.

#### **15. Involvement of third parties**

SWISSIGN may engage third parties at any time to perform its services.

#### **16. Warranty**

The SUBSCRIBER shall examine or arrange the examination of the material provided, including in particular the certificates provided, following their issuance and report any defects or incorrect and/or incomplete information promptly (within no more than 7 working days), and under all circumstances prior to the first usage. If evident defects are not reported promptly following receipt, and latent defects not promptly after discovery, the rights relating to defects shall be deemed to have been forfeited. The SUBSCRIBER shall bear the burden of proving the time when the defects objected to were discovered and that the report was made promptly.

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

SWISSIGN does not provide any warranty regarding the compatibility of the certificates provided with non-Swiss law and reserves the right to refuse requests for certificates from the SUBSCRIBER where these run contrary to statutory export restrictions or limitations or compliance requirements of SWISSIGN.

#### **17. Liability**

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

The liability provisions of the CP/CPS apply to third parties (see 3).

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

The SUBSCRIBER shall fully indemnify SWISSIGN from all third parties' claims resulting from use in breach of contract or unlawful or improper use of the CERTIFICATE SERVICE. The indemnification shall include also the obligation to hold SWISSIGN fully harmless against legal defence costs (e.g. procedural costs and legal fees).

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

In the event of personal injury, the Parties shall bear liability 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 provision.

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.

#### **18. Export and import, international use of certificates**

The SUBSCRIBER and the 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.swissign.com/export>).

The SUBSCRIBER and CERTIFICATE HOLDER acknowledges that the deployment and use of digital certificates and the exchange of digitally signed and/or encrypted data outside Switzerland, Liechtenstein and the EU/EEA is subject to foreign jurisdictions and that therefore different effects may result, which may be more or less extensive than is the case under Swiss, Liechtenstein or EU law.

The exchange of encrypted data and the export/import of cryptographic software or cryptographic data storage media are also subject to statutory restrictions in certain foreign countries. Clarification of matters in this respect shall be a matter under all circumstances for the SUBSCRIBER.

#### **19. Intellectual property rights**

No intellectual property rights (such as copyright, trademark, design or patent rights etc.) shall be transferred to the SUBSCRIBER by the CERTIFICATE SERVICE. All intellectual property rights over the material provided by SWISSIGN (documentation, devices, software etc.) shall remain the property of SWISSIGN or the third parties with rights thereto. In the event of the supply of material or executable

software, the SUBSCRIBER shall receive a non-exclusive, non-transferable licence to use such material in line with the contractual object, which shall be limited to the contractual term. The SUBSCRIBER shall not have any rights to make changes or further developments.

#### **20. Severability of this Agreement**

If individual terms of this SUBSCRIBER AGREEMENT are found to be invalid or unlawful, this shall not affect the validity of the Contract. Should this occur, the relevant term shall be replaced by a valid term that is commercially equivalent as far as possible.

#### **21. Amendment of the SUBSCRIBER AGREEMENT CERTIFICATE SERVICES**

SWISSIGN reserves the right to amend this Subscriber Agreement Certificate Services at any time. The relevant amended version shall be published on the website <https://www.swissign.com/en/cp-repository> in good time before it comes into effect and shall be notified through the system status page: <https://www.swissign.com/en/systemstatus>.

The amended SUBSCRIBER AGREEMENT shall be deemed to have been approved unless the SUBSCRIBER objects in writing within one month of the time it became aware of it. An objection shall be deemed to constitute notice of termination of the Contract and shall automatically result in its dissolution.

#### **22. Assignment and transfer of rights and duties**

The SUBSCRIBER may not assign or pledge any claims against SWISSIGN without the written consent of SWISSIGN.

The SUBSCRIBER shall not have the right to assign or transfer the rights and obligations pursuant to this Agreement.

### **23. 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.

### **24. Applicable law and jurisdiction**

The legal relationship resulting from this SUBSCRIBER AGREEMENT shall be governed exclusively by Swiss law. The above is subject to the law of Liechtenstein governing signatures for certificates that have been issued and signed by the Liechtenstein CA. 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.