

Subscriber Agreement / Terms of Service



Status: Final

Version: 1.0

OID: 47934.6.1.2.9.02

2019-04-16

Contents

1 History	1
2 Scope	1
3 Compliance with regulatory requirements	2
4 Contractual Components	2
5 Reissuing and change in attributes	2
6 Revocation of certificates	2
7 Certificate expiration	4
8 Directory service	4
9 Customer service, helpdesk, support	5
10 Duties of the SUBSCRIBER and CERTIFICATE HOLDER when dealing with certificates	5
10.1 Accuracy of information	5
10.2 Key generation	5
10.3 Protection of private key	5
10.4 Acceptance of certificate	5
10.5 Use of certificate	6
10.6 Duty to report and declaration of invalidity (revocation)	6
10.7 Termination of use of certificate	6
10.8 Response in the event of misuse	6
10.9 Revocation in the event of breaches of duty	7
10.10 OCSP Stapling	7
10.11 Particular compliance with the duty of care	7
11 Relevant information from WPIA	7

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	10
18 Export and import, international use of certificates	11
19 Intellectual property rights	11
20 Severability of this Agreement	11
21 Amendment of the SUBSCRIBER AGREEMENT CERTIFICATE SERVICES	12
22 Assignment and transfer of rights and duties	12
23 Out of court dispute resolution	12
24 Applicable law and jurisdiction	12

1 History

version	changes	approval date
1.0	initial document	2019-04-16

2 Scope

In applying for certificates and services that are based on the publicly trusted root certificates of the TERACARA CA, the Subscriber to a certificate service (hereafter SUBSCRIBER) consents to the Subscriber Agreement (hereafter SUBSCRIBER AGREEMENT). A SUBSCRIBER means an applicant for a TERACARA certificate, which acquires it from TERACARA 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 World Privacy and Identity Association (WPIA) - Verein zur Förderung von sicheren Technologien und Grundrechten im Internet, c/o realraum, Brockmannngasse 15, 8010 Graz, Austria (hereafter WPIA) concerning the usage of TERACARA certificates (hereafter referred to collectively as CERTIFICATE SERVICES).

A SUBSCRIBER MAY acquire certificate services either directly or through WPIA Cooperative eG - Genossenschaft zur Förderung von sicheren Technologien und Grundrechten im Internet.

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 <http://policy.wpia.club>.

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. WPIA Cooperative eG, employer of the Subscriber etc.).

The SUBSCRIBER acknowledges that no legal claims against WPIA MAY arise either under this SUBSCRIBER AGREEMENT or from the usage of the

CERTIFICATE SERVICE, unless WPIA contravenes any liability terms and conditions pursuant to section 17 “Liability”.

3 Compliance with regulatory requirements

Insofar as the issuance and management of certificates is subject to statutory requirements (e.g. eIDAS), WPIA warrants compliance with the relevant requirements and implementing provisions. WPIA SHALL in this regard be subject to oversight by the competent bodies (e.g. Austrian Telekom Control Commission) 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.

4 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 <http://policy.wpia.club>.

5 Reissuing and change in attributes

Reissuing/rekeying: The repeated issuance of certificates is not possible.

Any changes to the SAN attribute or subject SHALL require the certificate to be revoked and to issue a new one.

6 Revocation of certificates

Certificates that have been revoked MAY no longer be actively used and SHALL without exception be published as invalid in certificate revocation lists (“CRL”) and the online revocation service (“OCSP”).

Where appropriate, WPIA 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 WPIA 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 WPIA that the original certificate request was unauthorised and not approved or that the approval has been withdrawn.
- d) WPIA 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) WPIA 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) WPIA becomes aware of circumstances that suggest that the usage of a fully qualified domain name 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) WPIA 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) WPIA becomes aware of a change in the information contained in the certificate.
- i) WPIA 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 TERACARA or can no longer be valid on the basis of new regulations.
- j) WPIA takes the view that information contained in the certificate is imprecise or misleading.
- k) WPIA 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 WPIA to issue certificates that are compliant with the CA/Browser Forum Baseline Requirements has expired or is revoked or terminated and WPIA has not made provision to maintain the CRL/OCSP directories that are relevant for revocation.

- m) 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).
- n) A private key of the TERACARA 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.

WPIA 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. WPIA 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://TBD>.

7 Certificate expiration

The validity period of a TERACARA certificate is limited to the maximum remaining duration of the certificate of the issuing CA less 5 days. It SHALL be the sole responsibility of the Certificate Holder to ensure the uninterrupted usage of TERACARA certificates. For this reason, WPIA recommends to the SUBSCRIBER that it apply for a new certificate at least 30 days prior to the expiration of the certificate or commence the certificate renewal procedure at least 1 day prior to expiration of the certificate.

8 Directory service

WPIA 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 "TERACARA" on them as issuer. This enables people to infer that there is a contractual relationship between WPIA and the SUBSCRIBER or between WPIA and the CERTIFICATE HOLDER.

9 Customer service, helpdesk, support

WPIA operates a customer service unit (“Helpdesk” or “Support”). This MAY be reached by email at support@wpia.club. Any comments and feedback concerning this SUBSCRIBER AGREEMENT MAY also be submitted in this manner.

10 Duties of the SUBSCRIBER and CERTIFICATE HOLDER when dealing with certificates

10.1 Accuracy of information

The SUBSCRIBER and CERTIFICATE HOLDER represent and warrant that they will at all times provide WPIA 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 WPIA of them directly if they are in a direct commercial contractual relationship with WPIA, and otherwise SHALL notify WPIA through WPIA Cooperative eG in an adjustment to the order.

10.2 Key generation

If the SUBSCRIBER generate the key pair themselves, they 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.

10.3 Protection of private key

The SUBSCRIBER represent and warrant that they have taken all reasonable measures and that the CERTIFICATE HOLDER have exclusive control of the private keys. This includes all measures to keep the key confidential and protect it appropriately at all times.

10.4 Acceptance of certificate

The SUBSCRIBER undertake and warrant that they SHALL review the content of the certificate with the CERTIFICATE HOLDER upon receipt to check that

it is accurate.

10.5 Use of certificate

The SUBSCRIBER SHALL ensure that they install 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.

10.6 Duty to report and declaration of invalidity (revocation)

The SUBSCRIBER and the CERTIFICATE HOLDER SHALL ensure that the certificate is revoked immediately or ask WPIA 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, or
- c) if the private key can no longer be accessed.

10.7 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 become 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.

10.8 Response in the event of misuse

The SUBSCRIBER SHALL within the specified period carry out all of WPIA's instructions issued in relation to the theft of the private key.

When issuing its instructions WPIA SHALL consider ordinary office hours to the extent possible taking account of the urgency and SHALL endeavour to provide reasonable explanations for its instructions.

10.9 Revocation in the event of breaches of duty

The SUBSCRIBER and CERTIFICATE HOLDER acknowledge and accept that WPIA is authorised to revoke a certificate immediately if the SUBSCRIBER or CERTIFICATE HOLDER contravene the corresponding CP/CPS, or if WPIA 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 are not adhering to further statutory or contractual obligations, WPIA 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.

10.10 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.

10.11 Particular compliance with the duty of care

The SUBSCRIBER accept that any violation of their duties of care MAY result in financial loss and/or adverse consequences for WPIA 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.

11 Relevant information from WPIA

All relevant information relating to misuse, compromise, algorithm changes, system failures etc. SHALL be reported by WPIA through the system status page <https://TBD>.

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 WPIA against any counterclaims.

The following provisions SHALL apply in the event of non-payment WPIA Cooperative eG or SUBSCRIBER in relation to the CERTIFICATE SERVICE:

- a) If the SUBSCRIBER or WPIA Cooperative eG owes the service fee to WPIA, 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 retrieved through WPIA Cooperative eG, WPIA SHALL inform the SUBSCRIBER of WPIA Cooperative eG of the default on the part of the WPIA Cooperative eG.
- c) WPIA 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 nonpayment.

If payment is not made either by WPIA Cooperative eG or by the SUBSCRIBER before the final payment deadline, WPIA 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

WPIA 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 WPIA.

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 WPIA.

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, WPIA MUST retain all certificate holder data, documentation and audit information for a minimum period of 11 years after expiration of a certificate.

15 Involvement of third parties

WPIA 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, WPIA 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.

WPIA SHALL not provide any warranty regarding the compatibility of the certificates provided with non-Austrian 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 WPIA.

17 Liability

WPIA SHALL bear full liability towards the SUBSCRIBER for any losses occasioned by it to the SUBSCRIBER unless WPIA 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. WPIA SHALL not be liable for the systems and software used by the SUBSCRIBER.

The SUBSCRIBER SHALL fully indemnify WPIA 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 WPIA 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 Austrian Federal Act on Electronic Signatures and Trust Services for Electronic Transactions (Signature and Trust Services Act - SVG) and in Article 13 of the regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS-Regulation) 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://TBD>).

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 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 Austrian 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 WPIA (documentation, devices, software etc.) SHALL remain the property of WPIA 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

WPIA reserves the right to amend this Subscriber Agreement Certificate Services at any time. The relevant amended version SHALL be published on the website <http://policy.wpia.club> in good time before it comes into effect and SHALL be notified through the system status page: <https://TBD>.

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 WPIA without the written consent of WPIA.

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

All disputes or claims arising out of or in connection with this contract, including disputes relating to its validity, breach, termination or nullity, shall be submitted to the Arbitration Commission of the WPIA, and shall be finally settled under the Rules of Arbitration of WPIA by arbitrators appointed in accordance with the said rules.

24 Applicable law and jurisdiction

The legal relationship resulting from this SUBSCRIBER AGREEMENT SHALL be governed exclusively by Austrian law. The above is subject to the law of Austria governing signatures for certificates that have been issued and signed by the TERACARA 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 Graz, 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 Graz, Austria.