

This TunTrust subscriber agreement is entered into between:

- The national agency for digital certification - TunTrust and
- The subscriber, the individual or legal entity;
 - Identified in the subject name fields of an end user certificate; or
 - Responsible for the request, installation and maintenance of the systems on which a TunTrust TLS/SSL certificate is installed;
- The organisation with which TunTrust has contracted requesting the issuance of a certificate.

All subscribers must first read this agreement and agree, accept and be bound by its terms. If you do not accept the terms of this agreement, you are not authorised to be the subscriber of a TunTrust certificate and you must terminate your application or request revocation of such certificate.

This agreement incorporates by reference any certificate policies contained in the TunTrust certificate and conditions of the applicable root certificate policy/certification practice statement (“cp/cps”) located at <https://www.tuntrust.tn/repository>.

The use of a certificate signifies acceptance of that certificate. By accepting a certificate, the subscriber acknowledges that they agree to the terms and conditions contained in this subscriber agreement and the cp/cps.

Capitalized terms not defined in this agreement have the meaning specified in the cp/cps. *

TUNTRUST and the SUBSCRIBER, intending to be legally bound, agree as follows:

1- Issuance; Fees: Upon the Subscriber's submission of a completed Application and TunTrust's acceptance of that Application, TunTrust shall issue the number of Certificates applied for by the Subscriber. The Subscriber shall pay the then-current published or contractually agreed upon price for such Certificate(s) before issuance.

2- Use, Purpose and Limitations: The Subscriber shall use the TunTrust Certificate in accordance with the terms and conditions of the CP/CPS.

3- Role and Obligations of TunTrust: TunTrust shall act as the Certification Authority for the TunTrust Certificate and perform its obligations as specified in this Agreement and the CP/CPS. TunTrust is not responsible or liable for the cryptographic methods used in connection with the TunTrust Certificate. TunTrust represents and warrants that it has followed the requirements of the CP/CPS in issuing the Certificate and in verifying the accuracy of the information contained in the Certificate.

4- Role and Obligations of the Subscriber: Before accepting and using a TunTrust Certificate, the Subscriber must: (i) where applicable, generate its own Key Pair; (ii) submit an application for a TunTrust Certificate; and (iii) accept and agree to the terms of this Agreement. The Subscriber is solely responsible for the security protection of the Private Key underlying the TunTrust Certificate.

So long as the Certificate is valid, the Subscriber hereby gives his/her acceptance to the following responsibilities

- Having a basic understanding of the proper use of public key cryptography and certificates;
- Providing only correct information without errors, omissions or misrepresentations;
- Substantiating information by providing a properly completed and personally signed Order form;
- Supplementing such information with a proof of identity and the provision of the information as specified in the CP/CPS;
- Verifying the content of a newly issued certificate before its first use and to refrain from using it, if it contains misleading or inaccurate information.
- Reading and agreeing to all terms and conditions of the CP/CPS and other relevant regulations and agreements;
- Ensuring complete control over the private key by not sharing private keys and passwords;
- Notifying TunTrust of any change to any of the information included in the certificate or any change of circumstances that would make the information in the certificate misleading or inaccurate;

- Invalidating the certificate immediately if any information included in the certificate is misleading or inaccurate, or if any change of circumstances, makes the information in the certificate misleading or inaccurate;
- Notifying TunTrust immediately of any suspected or actual compromise of the private key and requesting that the certificate be revoked;
- Immediately ceasing to use the certificate upon (a) expiration or revocation of such a certificate, or (b) any suspected or actual damage/corruption of the private key corresponding to the public key in such a certificate, and immediately removing such a certificate from the devices and/or software onto which it has been installed;
- Refraining to use the subscriber's private key that corresponds to the public key certificate to sign other certificates;
- If the Certificate requires the use of a Qualified Electronic Signature Creation Device (QSCD) or Cryptographic Module, for example for the creation of digital signatures, the Subscriber must use the Certificate with such a device that either been supplied by or approved by TunTrust;
- If the Subscriber generates their keys, then they will generate them in a secure manner in accordance with industry leading practices;
- Protecting the private key from unauthorized access.

The Subscriber shall indemnify and hold harmless TunTrust from any and all damages and losses arising out of: (i) use of a TunTrust Certificate in a manner not authorised by TunTrust; (ii) tampering with a TunTrust Certificate; or (iii) any misrepresentations made during the use of a TunTrust Certificate. In addition, the Subscriber shall indemnify and hold harmless TunTrust from and against any and all damages (including legal fees) for lawsuits, claims or actions by third-parties relying on or otherwise using a TunTrust Certificate relating to: (i) the Subscriber's breach of its obligations under this Agreement or the CP/CPS; (ii) the Subscriber's failure to protect its Private Key; or (iii) claims (including without limitation infringement claims) pertaining to content or other information or data supplied by the Subscriber.

5- Revocation: TunTrust revokes a Certificate within 24 hours if one or more of the following occurs:

- a) The Subscriber requests in writing that TunTrust revoke the Certificate;
- b) The Subscriber notifies TunTrust that the original certificate request was not authorized and does not retroactively grant authorization;
- c) TunTrust obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of the CP/CPS;
- d) TunTrust obtains evidence that the Certificate was misused;
- e) TunTrust is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
- f) TunTrust is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- g) TunTrust is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- h) TunTrust is made aware of a material change in the information contained in the Certificate;
- i) TunTrust is made aware that the Certificate was not issued in accordance with the applicable CP/CPS;
- j) TunTrust determines that any of the information appearing in the Certificate is inaccurate or misleading;

- k) TunTrust ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- l) TunTrust's right to issue Certificates under these Requirements expires or is revoked or terminated, unless TunTrust has made arrangements to continue maintaining the CRL/OCSP Repository;
- m) TunTrust is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
- n) Revocation is required by the TunTrust's CP/CPS; or
- o) The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).
- p) if the Subscriber (or his representative) did not present himself to retrieve his ID-Trust certificate (digital signature certificate) from TunTrust CRA or any PVP within 90 calendar days from the date of generation of this certificate, TunTrust reserves the right to revoke this certificate without any prior notice. The Subscriber whose certificate has been revoked under these conditions, can file a new certificate request at no additional cost using an invoice provided by TunTrust.

6- Disclaimer of warranties: To the extent permitted by applicable law, CP/CPS, the Subscriber Agreement, the Relying Party Agreement, the Issuing CA Agreement, the Registration Authority Agreement and any other contractual documentation applicable within the TunTrust PKI shall disclaim TunTrust ' possible warranties, including any warranty of merchantability or fitness for a particular purpose.

To the extent permitted by applicable law, TunTrust makes no express or implied representations or warranties pursuant to CP/CPS. TunTrust expressly disclaims any and all express or implied warranties of any type to any person, including any implied warranty of title, non infringement, merchantability, or fitness for a particular purpose.

7- Limitation of liability and damages: TunTrust is only liable for damages which are the result of its failure to comply with CP/CPS and which were provoked deliberately or wantonly negligent.

- TunTrust is not in any event be liable for any loss of profits, indirect and consequential damages, or loss of data, to the extent permitted by applicable law. TunTrust is not liable for any damages resulting from infringements by the Subscriber or the Relying Party on the applicable terms and conditions.

- TunTrust is not in any event be liable for damages that result from force major events as detailed in the CP/CPS. TunTrust takes commercially reasonable measures to mitigate the effects of force major in due time. Any damages resulting of any delay caused by force major will not be covered by TunTrust.

- The Subscriber is liable to TunTrust and Relying Parties for any damages resulting from misuse, willful misconduct, failure to meet regulatory obligations, or noncompliance with other provisions for using the certificate.

8- Third-Party Beneficiaries: All application software and operating system vendors with whom TunTrust has entered into a contract for inclusion of the TunTrust Root Certificate as a trusted root Certificate in their software and all relying parties who actually rely on such Certificate during the period when the Certificate is valid are intended third party beneficiaries of this Agreement.

9- Term & Termination: This Agreement is effective upon TunTrust' acceptance of the Subscriber's Application, and will terminate, except for those provisions which by their nature survive termination, upon the earliest of: (i) the latest expiration date of the TunTrust Certificates issued to You under this Agreement; (ii) a breach of the Subscriber's obligations under this Agreement; (iii) the Subscriber's written request; or (iv) revocation of all TunTrust Certificates issued to You under this Agreement.

10- Governing Law: This Subscriber Agreement is governed, construed and interpreted in accordance with the laws of Tunisia. This choice of law is made to ensure uniform interpretation of CP/CPS, regardless of the place of residence or place of use of TunTrust Certificates or other products and

services. The law of Tunisia applies also to all TunTrust commercial or contractual relationships in which CP/CPS may apply or quoted implicitly or explicitly in relation to TunTrust products and services where TunTrust acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including TunTrust partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Ariana, Tunisia.

11- Personal data protection

TunTrust fully respects the Tunisian law on the protection of personal data and any other applicable law in Tunisia.

Any subscriber information that is not made public through Certificates issued by TunTrust is considered private information. Any information made public in a certificate issued by TunTrust or by a publicly available service provided by TunTrust shall not be considered confidential.

TunTrust retains all Certificate lifecycle events for at least 20 years after any certificate based on these records ceases to be valid.

12- Refund policy

TunTrust does not refund the fees of certificates after issuance except for the case p) of Article 05 "Revocation".

13- Notices: All notices provided by the Subscriber are considered given when in writing and delivered in hand by independent courier, delivered by registered or certified mail-return receipt requested, or sent by facsimile with receipt confirmed by telephone or other verifiable means, to:

The National Agency for Digital Certification,

Address: TUNTRUST - National Agency for Digital Certification
Technopark El Ghazala, Road of Raoued, Ariana, 2083, Tunisia.

Tel: +216 70 834 600

Fax: +216 70 834 555

E-mail address: pki@tuntrust.tn

Website: www.tuntrust.tn

14- Certificate Transparency: To ensure Certificates function properly throughout their lifecycle, TunTrust may log SSL Certificates with a public certificate transparency database. Because this will become a requirement for Certificate functionality, Subscriber cannot opt out of this process. Log server information is publicly accessible. Once submitted, information cannot be removed from a log server.

**THE SIGNATURE THIS AGREEMENT FORM SHOWS THE SUBSCRIBER'S
ACKNOWLEDGMENT AND SUBSCRIBER ACCESSION TO THESE TERMS AND CONDITIONS
OF USE AND THE PROCEDURES ON THE WWW.TUNTRUST.TN WEBSITE AND ITS CONSENT
FOR THE USE OF ITS DATA A PERSONAL CHARACTER FOR THE GENERATION OF THE
REQUESTED CERTIFICATE.**

NAME, FIRST NAME AND SIGNATURE