IMPORTANT

Please read this TunTrust - Subscriber Agreement carefully before applying for, accepting, or using a TunTrust SSL Certificate.

This TunTrust Certificate Subscriber Agreement (this "Agreement") is between the individual or legal entity identified on the issued Certificate(s) resulting from this Agreement ("Subscriber") and Agence Nationale de Certification Electronique of Tunisia - TunTrust. This Agreement governs the Subscriber's application for and use of a Certificate issued from TunTrust. The use of a Certificate implies the acceptance of that Certificate.

TUNTRUST and the SUBSCRIBER agree as follows:

1 DEFINITIONS

- **Applicant:** The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate request.
- **Baseline Requirements:** The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates as published by the CA/Browser Forum and any amendments to such document.
- **Certificate:** An electronic document that uses a digital signature to bind a public key and an identity.
- **Certificate Policy (CP):** A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
- **Certificate Revocation List (CRL)**: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
- **Certification Authority:** An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.
- **Certification Practice Statement:** One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
- **Domain Label:** From RFC 8499 (<http://tools.ietf.org/html/rfc8499>): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."
- **Domain Name:** An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.
- **Domain Name Registrant:** Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
- **Domain Name Registrar:** A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).
- **Expiry Date:** The "Not After" date in a Certificate that defines the end of a Certificate's validity period.
- **Fully-Qualified Domain Name:** A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.
- **Individual:** A natural person.
- **IP Address:** A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.
- **Key Compromise**: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it
- **Key Pair:** The Private Key and its associated Public Key.
- **Legal Entity**: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
- **OCSP Responder:** An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
- **Online Certificate Status Protocol (OCSP):** An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

- **Private Key:** The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
- **Public Key:** The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
- **Registered Domain Name:** A Domain Name that has been registered with a Domain Name Registrar.
- **Registration Authority (RA):** Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the Certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
- **Relying Party:** Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate. Relying Parties must read and agree to TunTrust's relying party agreement available at https://www.tuntrust.tn/repository.
- **Repository:** An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
- **Subscriber:** A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement.
- **Subscriber Agreement:** An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties available at https://www.tuntrust.tn/repository.
- **Terms of Use:** Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.
- **Valid Certificate:** A Certificate that passes the validation procedure specified in RFC 5280.
- **Validity Period:** The validity period is as defined within RFC 5280, Section 4.1.2.5: the period of time from notBefore through notAfter, inclusive.
- **Wildcard Certificate:** A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names contained in the Certificate.
- **Wildcard Domain Name:** A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

2 ISSUANCE FEES

The fees for registering and issuing an SSL Certificate are publicly available on TunTrust website https://www.tuntrust.tn/ .

Upon the Applicant's submission of a completed Application of an SSL Certificate and TunTrust's acceptance of that application, the Subscriber shall pay all applicable fees for the Certificate before the requested Certificate is issued.

After the issuance of the Certificate, no other fees will be applied for the use of the SSL Certificates.

None of the fees collected are refundable.

3 USE, PURPOSE AND LIMITATIONS

The TunTrust OV SSL Certificates are used to secure online communication and transactions. The OV SSL Certificate allows the end entity to prove its identity to other participants and maintain the integrity of the transaction.

The Certificate will be valid during the entire Validity Period indicated in the Certificate, unless revoked earlier. This Agreement will remain in force during the entire period during which the Certificate is valid and will terminate once the Subscriber Certificate expires or is revoked.

4 ROLE AND OBLIGATIONS OF THE SUBSCRIBER

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

The Subscriber warrants:

a) Accuracy of Information: to provide accurate and complete information at all times to TunTrust, both in the Certificate request and as otherwise requested by TunTrust in connection with the issuance of the Certificate(s) to be supplied by TunTrust;
b) Protection of Private Key: to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
c) Acceptance of Certificate: to review and verify the Certificate contents for accuracy;
d) Use of Certificate: to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement;
e) Reporting and Revocation: to: (i) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (ii) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate ;
f) Termination of Use of Certificate: to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise ;
g) Responsiveness: to respond to TunTrust's instructions concerning Key Compromise or Certificate misuse within a specified time period ;
h) Acknowledgment and Acceptance: to have acknowledged and accepted that TunTrust is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or if revocation is required by the "TunTrust PKI CP/CPS", or the CA/B Forum Baseline Requirements.

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 using TunTrust revocation online service available at https://www.tuntrust.tn/Revocation-online-service or through physical presence before a TunTrust RA operator;
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;
d) TunTrust is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); or
e) TunTrust obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

TunTrust revokes a Certificate within 5 days if one or more of the following occurs:

a) The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of "TunTrust PKI CP/CPS" regarding Key Pairs;
b) TunTrust obtains evidence that the Certificate was misused;
c) TunTrust is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
d) TunTrust is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address 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);
e) TunTrust is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
f) TunTrust is made aware of a material change in the information contained in the Certificate;
g) TunTrust is made aware that the Certificate was not issued in accordance with the Baseline Requirements or the "TunTrust PKI CP/CPS";
h) TunTrust determines or is made aware that any of the information appearing in the Certificate is inaccurate;

i) TunTrust's right to issue Certificates under the CA/B Forum Baseline Requirements expires or is revoked or terminated, unless TunTrust has made arrangements to continue maintaining the CRL/OCSP Repository;
j) Revocation is required by the TunTrust PKI CP/CPS; or
k) TunTrust is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed.

A Certificate may be revoked for the following reasons. If the situation is that multiple revocation reasons apply, the revocation reason of higher priority (as per the order of the following list) should be indicated:

a) keyCompromise (RFC 5280 CRLReason #1): The Certificate Subscriber must choose the "keyCompromise" revocation reason when they have reason to believe that the private key of their Certificate has been compromised, e.g. an unauthorized person has had access to the private key of their Certificate.
b) cessationOfOperation (RFC 5280 CRLReason #5): The Certificate Subscriber should choose the "cessationOfOperation" revocation reason when they no longer own all of the domain names in the Certificate or when they will no longer be using the Certificate because they are discontinuing their website.
c) affiliationChanged (RFC 5280 CRLReason #3): The Certificate Subscriber should choose the "affiliationChanged" revocation reason when their organization's name or other organizational information in the Certificate has changed.
d) superseded (RFC 5280 CRLReason #4): The Certificate Subscriber should choose the "superseded" revocation reason when they request a new Certificate to replace their existing Certificate.
e) No reason provided or unspecified (RFC 5280 CRLReason #0): When the reason codes above do not apply to the revocation request, the Subscriber must not provide a reason other than "unspecified".

6 DISCLAIMER OF WARRANTIES

To the extent permitted by the applicable law, the Subscriber Agreement and any other applicable contractual agreement, TunTrust makes no express or implied representations or warranties pursuant to the “TunTrust PKI 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 the “TunTrust PKI CP/CPS” and which were provoked deliberately or wantonly negligent.

TunTrust is not in any event liable for any loss of profits, indirect and consequential damages, or loss of data, to the extent permitted by the Tunisian law. TunTrust is not liable for any damages resulting from infringements by the Subscriber 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 “TunTrust PKI 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 PRIVACY AND 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.

9 INDEMNIFICATION

To the extent permitted by the applicable law, each Subscriber shall release, indemnify and hold harmless TunTrust CA, and all TunTrust directors, shareholders, officers, agents, employees, contractors and successors of the foregoing, against any loss, damage, or expense, including reasonable attorney’s fees, related to (i) any misrepresentation or

omission by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of its Subscriber Agreement, the "TunTrust PKI CP/CPS", or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of a Certificate or Private Key.

10 AMENDMENTS

TunTrust may amend this Agreement, the "TunTrust PKI CP/CPS", its website, and any documents listed in its Repository (https://www.tuntrust.tn/repository) at any time by posting either the amendment or the amended document in the Repository. The Subscriber shall periodically review the Repository to be aware of any changes. The Subscriber may terminate this Agreement if the Subscriber does not agree to the amendment. The Subscriber's continued use of the Certificate after an amendment is posted, constitutes the Subscriber's acceptance of the amendment.

11 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.

12 NOTICES

The Subscriber shall send all notices to TunTrust by mail in writing with return receipt requested,
to :
Agence Nationale de Certification Electronique,
Address: TUNTRUST - Agence Nationale de Certification Electronique , Technopark El Ghazala, Road of Raoued, Ariana, 2083, Tunisia.

You agree that by applying for, accepting, or using a TunTrust SSL Certificate, you acknowledge that you have read this Agreement, that you understand it, and that you agree to its terms. If you are applying for, accepting, or using a TunTrust SSL Certificate on behalf of a company or other legal entity, you represent that you are an authorized representative of such entity and have the authority to accept this agreement on such entity's behalf. If you do not have such authority or if you do not accept this Agreement, do not apply for, accept, or use a TunTrust SSL Certificate.

SURNAME, GIVEN NAME AND SIGNATURE