PKI Disclosure Statement of TnTrust Sign PKI

Agence Nationale de Certification Electronique

Review

Version	Date	Comment	Section/Page
00	23 September 2022	1st version	All pages
01	17 October 2023	2nd version	No Changes
01.1	14 October 2024	3rd revision	Sections 7 & 10

Table of Contents

1. Notice

This document is the PKI Disclosure Statement, hereinafter referred to as the PDS, of TunTrust, the Agence Nationale de Certification Electronique in Tunisia. This document does not substitute or replace the Certificate Policy nor the Certification Practice Statement (CP/CPS) of TnTrust Sign PKI, under which TunTrust ID-Trust Certificates are issued.
This statement, which follows the structure of Annex A of the document ETSI EN 319 411-1, is merely informative and in no way replaces the provisions of the aforementioned documents.

2. Contact Information

All notices 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 Agence Nationale de Certification Electronique
Address: TUNTRUST - Agence Nationale de Certification Electronique
Technopark El Ghazala, Road of Raoued, Ariana, 2083
Tunisia.
Tel: +216 70 834 600
E-mail address: pki@tuntrust.tn
Website: https://www.tuntrust.tn

Subscribers, Relying Parties, Application Software Suppliers, and other third parties can submit Certificate Problem reports of suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates via email to: revoke@tuntrust.tn. Further details are available in https://www.tuntrust.tn/content/revocation-certificat.

3. Certificate type, Validation procedures and Usage

3.1. Certificate type and usage

The end-user Certificates issued under the ***TnTrust Sign PKI*** are ID-Trust Certificates.
An ID-Trust Certificate is an authentication and digital signing Certificate on a QSCD for natural person with or without professional attributes, that is compliant with ETSI EN 319 411-2.
The ID-Trust Certificates have the following OIDs:

0.4.0.2042.1.2
2.16.788.1.2.7.1.2.1.1

3.2. Validation procedures

In order to ease Subscriber registration preparation and to reduce the amount of errors, an end-user web-based registration interface is provided to the Subscriber at https://ecert.tuntrust.tn. It requires users to maintain accounts with a suitably strong username and password for ongoing maintenance of the lifecycle of the Certificate.

The interface presents the Subscriber with an electronic form to collect information needed for registration. This form will dynamically present appropriate fields.

The legal representative of a Legal Entity registers on the registration web interface by providing the requested documents as detailed in Section 3.2.2.1. The legal representative must then designate one or two certification agents. A contractual agreement cosigned between the legal representative and the Certification agent must be uploaded to the web interface at https://ecert.tuntrust.tn to assert the designation of the Legal Entity's certification agent by the legal representative.

The Certification Agent has to provide the requested documents in section 3.2.2.1 of the CP/CPS of TnTrust Sign PKI and initiate Certificate Requests for Applicants who are Individuals affiliated with the Legal Entity.

After email control verification as detailed in section 3.2.5 of the CP/CPS of TnTrust Sign PKI, the Applicant is prompted to change the password of the account on the registration web interface. Upon successful login to the interface, the Applicant must fill in the online order form, submit the requested documents in section 3.2.2.1 of the CP/CPS of the TnTrust Sign PKI, accept the displayed Subscriber Agreement, choose a RapidPost Agency (or its equivalent in other countries) for Certificate provisioning and submit the Certificate Request to TunTrust.

The Certification Agent has to pay the fees of the Certificate requests at the registration web interface for these Certificate requests to be transmitted to validation by a TunTrust RA operator.

A TunTrust RA operator checks that the Application includes all requested documents in section 3.2.2.1 of the CP/CPS of the TnTrust Sign PKI and that these documents are acceptable and authentic. For Tunisian entities, a verification tool based on webservices of governmental entities that meet the requirements of section 3.2.2.7 of the CP/CPS of the TnTrust Sign PKI, is at the disposal of the RA operator to check the authenticity of the provided information.

Upon successful verification of Certificate Application, the RA operator initiates a certificate signing request using multi-factor authentication.

Key generation is performed under TunTrust's direct control. Private Keys are generated directly on compliant Qualified Signature Creation Devices (QSCD). Certificate enrollment requests are sent to the issuing CAs as signed and encrypted messages over a HTTPS link.

After the issuance of the Certificate by the "TnTrust CA – QSign1", the RA operator authorizes the system to install the Certificate in a QSCD. A PIN code is then automatically sent by email to the Subscriber.

The QSCD is put in an envelope that holds a tracking number and are collected by a RapidPost Agent to be shipped to the RapidPost Agencies chosen by the Applicants.

The tracking number is automatically sent by email to the Subscriber.

4. Reliance limits

The TnTrust Qualified Gov CA does not set reliance limits for Certificates issued under the CP/CPS of the TnTrust Sign PKI. Reliance limits may be set by other policies, application controls and Tunisia applicable law or by Relying Party Agreement.

TunTrust records details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the Certificate request; the time and date; and the personnel involved.

TunTrust retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least 20 years after any Certificate based on that documentation ceases to be valid.

5. Obligations of subscribers

Before accepting and using a TunTrust Certificate, the Subscriber must: (i) submit a certificate request for a TunTrust Certificate; and (ii) accept and agree to the terms and conditions in the Subscriber Agreement. By accepting the Subscriber Agreement, the Subscriber agrees with and accepts Subscriber Agreement and the applicable CP/CPS.

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

1. **Accuracy of Information:** An obligation and warranty 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;
2. **Protection of Private Key:** An obligation and warranty by the Applicant 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);
3. **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of Certificate:** An obligation and warranty to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement;
5. **Reporting and Revocation:** An obligation and warranty to: (a) 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 (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.
6. **Termination of Use of Certificate:** An obligation and warranty 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.

7. **Responsiveness:** An obligation to respond to TunTrust's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. **Acknowledgment and Acceptance:** An acknowledgment and acceptance 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 present CP/CPS, or the CA/B Forum Baseline Requirements.

6. Certificate status checking obligations of relying parties

Each Relying Party represents that, prior to relying on a TunTrust Certificate, it:

1. Obtained sufficient knowledge on the use of digital Certificates and PKI,
2. Studied the applicable limitations on the usage of Certificates and agrees to TunTrust's limitations on liability related to the use of Certificates,
3. Has read, understands, and agrees to this CP/CPS,
4. Verified both the TunTrust Certificate and the Certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use a TunTrust Certificate if the Certificate has expired or been revoked, and
6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a TunTrust Certificate after considering:
   a) applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
   b) the intended use of the Certificate as listed in the Certificate or this CP/CPS,
   c) the data listed in the Certificate,
   d) the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
   e) the Relying Party's previous course of dealing with the Subscriber,
   f) the Relying Party's understanding of trade, including experience with computer-based methods of trade, and
   g) any other indication of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a Certificate is at a party's own risk.

Relying Parties must use online resources that TunTrust makes available through its repository to check the status of a Certificate before relying on it.

TunTrust updates OCSP, CRLs and the LDAP directory accordingly at the following URLs:

- CRLs are available https://www.tuntrust.tn/repository
- OCSP service is available from http://va.tuntrust.tn
- LDAP directory is available on ldap://ldap.tuntrust.tn and on the web interface https://www.tuntrust.tn/repository

7. Limited warranty and disclaimer/Limitation of liability

TunTrust is only liable for damages which are the result of its failure to comply with this 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 liable for damages that result from force major events as detailed in Section 9.5 in the CP/CPS of TnTrust Sign PKI. 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.
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 applicable 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 except for the ID-Trust as follows: If the Subscriber identifies that the cryptographic support is Defective[i] within 45 days of the expedition date of their Certificate, they are entitled to request a replacement from TunTrust free of charge.

8. Applicable agreements, CPS and CP

The TunTrust CP/CPS and the Subscriber Agreement can be found on the website of TunTrust at https://www.tuntrust.tn/repository.

9. Privacy Policy

TunTrust protects personal information in accordance with the Tunisian law N° 2004-63 of July 27th, 2004 on the protection of personal data and TunTrust internal document.
TunTrust makes available to Subscribers and Relying Parties its Privacy Policy on the website https://www.tuntrust.tn/repository .

10. Refund Policy

TunTrust does not refund the fees of Certificates.

11. Applicable law, complaints and dispute resolution

This governed, construed and interpreted in accordance with the laws of Tunisia. This choice of law is made to ensure uniform interpretation of this PDS, regardless of the place of residence or place of use of TunTrust Certificates. The law of Tunisia applies also to all TunTrust commercial or contractual relationships in which this 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 in Tunisia.

12. CA and Repository licenses, trust marks and audit

An annual audit is performed by an independent external auditor to assess TunTrust's compliance with standards set forth above.

An audit period must not exceed one year in duration. In addition to that, more than one compliance audit per year is possible if this is requested by TunTrust or is a result of unsatisfactory results of a previous audit.

TunTrust's audit is performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.1 of the CA/B Forum Baseline Requirements);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function; and
4. accredited in accordance with ISO17065 applying the requirements specified in ETSI EN 319 403;
5. Bound by law, government regulation, or professional code of ethics.

- [i] **Defective**: A cryptographic support is considered defective by TunTrust if it presents one or more of the following aspects:
  - The support cannot properly store or protect cryptographic keys in accordance with the technical specifications in the corresponding CP/CPS.
  - The cryptographic support can no longer be accessed or used with compatible devices or software, despite attempts to reset the password or unlock it using the tools provided by TunTrust.