Tunisian National PKI

PKI Disclosure Statement of the TnTrust Qualified Gov CA

Agence Nationale de Certification Electronique

Review

Version	Date	Comment	Section/Page
00	15/02/2017	1st version	All pages
01	31/08/2018	first revision	All pages
02	16/09/2019	2nd revision	All pages
02.1	13/01/2020	3rd revision	First Page

	Author	Validated by	Approved by
Entity :	TunTrust	Steering comity of Integrated Management System	TunTrust Board of Directors
Date :	26 November 2019	10/01/2020	10/01/2020

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) under which TunTrust certificates are issued.
This statement, which follows the structure of Annex A of the document ETSI EN 319411-1, 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

The form to be used for applying for the revocation of a certificate can be obtained from the following URL: https://www.tuntrust.tn/fr/content/revocation-certificat.

3. Certificate type, Validation procedures and Usage

3.1. Certificate type and usage

The description of each class/type of certificate issued by the CA, corresponding validation procedures, and any restrictions on certificate usage is presented below:

End User Certificates issued by ***TnTrust Qualified Gov CA***:

Service	Description	OID
ID-Trust	An authentication and digital signing Certificate on a QSCD for natural person, that is compliant to ETSI EN 319 411-2.	QCP-n-QSCD OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.1
ID-Trust Pro	An authentication and digital signing Certificate on a QSCD for natural person with professional attributes, that is compliant to ETSI EN 319 411-2.	QCP-n-QSCD OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.1
Enterprise-ID	Qualified certificates for electronic seal (eSeal) issued to legal persons or public authorities, that is compliant to ETSI EN	QCP-l-QSCD OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.2

	319 411-1.	
DigiGO	An authentication and digital signing Certificate on a remote QSCD for natural person, that is compliant to ETSI EN 319 411-2.	QCP-n-QSCD OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.3
DigiGO Pro	An authentication and digital signing Certificate on a remote QSCD for natural person with professional attributes, that is compliant to ETSI EN 319 411-2.	QCP-n-QSCD OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.3

3.2. Validation procedures

TunTrust delegates the performance of its functions to Delegated Registration Authorities (DRAs) that have to abide by all the requirements of the DRA agreement and the CP/CPS. DRAs may, however implement more restrictive practices based on their internal requirements.

The Delegated Registration Authorities (DRAs) aim to operate one or several PVPs and VVSs and proceed, under strictly determined and controlled conditions, to the validation of an Applicant's identity through:

- physical face-to-face identification,

  or

- video identification that provide equivalent assurance in terms of reliability to the physical presence.

Any DRA can delegate, in the Physical Verification Points (PVPs) or the Video Verification Services (VVSs), the Applicant's identity verification function and the receipt of documentation and, if applicable, the compiling of documentation and verification of its suitability as well as the delivery of the cryptographic device.

Based on the documentation collected by the PVP or the VVS, the DRA operator checks the documentation and, if applicable TunTrust CA issues the certificate with no need to carry out a new identity verification.

4. Reliance limits

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

TunTrust and each Delegated Third Party record 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.
TunTrust retains any audit logs generated for at least seven years.

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 signing the Subscriber Agreement, the Subscriber agrees with and accepts the associated 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 TunTrust discovers that the

Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

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 the CP/CPS of Tunisian National PKI,
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 the CP/CPS of Tunisian National PKI,
    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.

In order to be a Relying Party, a Party seeking to rely on a Certificate issued by TunTrust CAs agrees to and accepts the Relying Party Agreement (available on https://www.tuntrust.tn/repository) by querying the existence or validity of; or by seeking to place or by placing reliance upon a Certificate.

Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

- The appropriateness of the use of the Certificate for any given purpose and that the use is not prohibited by this CP/CPS.
- That the Certificate is being used in accordance with its Key-Usage field extensions.

- That the Certificate is valid at the time of reliance by reference to Online Certificate Status Protocol or Certificate Revocation List checks

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 from https://crl.tuntrust.tn and https://www.tuntrust.tn/repository
- OCSP service is available from https://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 the 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. Applicable agreements, CPS and CP

The TunTrust CP/CPS, the Subscriber Agreement and the Relying Party 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 treats all personal information about an individual that is not publicly available in the contents of a Certificate, CRL or OCSP as private information. TunTrust protects private information using appropriate safeguards and a reasonable degree of care.

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 except for when an ID-Trust certificate of a subscriber who did not retrieve his/her certificate within 90 calendar days from the date of notification of the issuance of the said certificate, was revoked. In the latter case, an invoice is provided to the subscriber in order to submit a new certificate application with no additional fees.

11. Applicable law, complaints and dispute resolution

This PDS is 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 the TunTrust 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 the TnTrust Qualified Gov CA's compliance with standards set forth in the Tunisian National PKI CP/CPS.
An audit period must not exceed one year in duration. 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 of the CP/CPS of the Tunisian National PKI);
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;
4. accredited in accordance with ISO17065 applying the requirements specified in ETSI EN 319 403; and
5. Bound by law, government regulation, or professional code of ethics.