National Agency For Digital Certification

PKI Disclosure Statement of the TnTrust Gov CA

Review

Rev	Date	Comment	Page
00	15/02/2017	1st version	All pages
01	31/08/2018	first revision	All pages

	Author	Validated by	Approved by
Entity :	TunTrust	Steering comity of Integrated Management System	TunTrust Board of Directors
Date :	30/08/2018	31/08/2018	31/08/2018

Table of Contents

1. Notice

This document is the PKI Disclosure Statement, hereinafter referred to as the PDS, of TunTrust, the National Agency For Digital Certification 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 National Agency for Digital Certification,
Address: TUNTRUST - National Agency for Digital Certification
Technopark El Ghazala,Road of Raoued, Ariana, 2083
Tunisia.E-mail: ndca.pki@tuntrust.tn
Tel: +216 70 834 600
Fax: +216 70 834 555
E-mail address: ndca.pki@tuntrust.tn
Website: www.tuntrust.tn

3. Certificate type, Validation procedures and Usage

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	Intended usage	OID
ID-Trust Certificate	ID-Trust certificate is used to sign document. It is also used for authentication purposes. ID-Trust certificate contains the validated email address, the applicant's verified data and, if the organization entry option has been selected, the verified data of the organization. ID-Trust certificate is a hardware-based certificate and is issued for periods of 1 year or 2 years.	qcp-n-qscd OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.1
Enterprise ID Certificate	Enterprise ID certificate is used to	qcp-l-qscd

	create qualified electronic seals. Enterprise ID certificate contains the verified data of the organization. Enterprise ID certificate is a hardware-based certificate and is issued for periods of 1 year or 2 years.	OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.2

Validation procedures

In all the cases, the Subscriber must appear in person before a Registration Authority of TunTrust or a Physical Verification Point (PVP), which will confirm the personal data on his/her ID card and the fact that he/she appeared in person. All information contained in the application shall be controlled with reference to the ID card. The examination complies with the requirements of the CA Browser Forum.

4. Reliance limits

The TnTrust Qualified Gov CA does not set reliance limits for Certificates issued under this policy. Reliance limit may be set by other policies, application controls and Tunisia applicable law or by Relying Party Agreement.

In order to manage operation of TunTrust system and supervise TunTrust users and personnel efficiently, all events occurring in the system and having essential impact on TunTrust security and all events relating to the life cycle of keys managed by the CA, including any subject key pairs generated by the CA are recorded.

5. Obligations of subscribers

Before accepting and using a TunTrust Certificate, the Subscriber must: (i) submit an application for a TunTrust Certificate; and (ii) 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.

6. Certificate status checking obligations of relying parties

Within its CP/CPS, TunTrust provides the conditions under which Certificates may be relied upon by Relying Parties including the appropriate Certificate services available to verify Certificate validity such as CRL and/or OCSP.

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

Authorized 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.

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 can be found on the website of TunTrust at https://www.tuntrust.tn/repository.

As for the Subscriber Agreement and the Relying Party Agreement, they may be found on the website of TunTrust at http://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 or CRL as private information. TunTrust protects private information using appropriate safeguards and a reasonable degree of care.

10. Refund Policy

TunTrust does not refund the fees of certificates after issuance.

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 or other products and services. 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, 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 CA WebTrust/ETSI standards.

More than one compliance audit per year is possible if this is requested by the audited party or is a result of unsatisfactory results of a previous audit.

The TunTrust's CAs compliance audits are performed by a public accounting firm that:

- Demonstrates proficiency in conducting the ETSI for Certification Authorities,
- Demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function,
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme,
- Is bound by law, government regulation or professional code of ethics.