



POLICY

PKI Disclosure Statement of TnTrust Corporate CA

Code : PL/TC/11
Rev : 00
Date : 15/02/2017
Page : 1/7
NC: PU

National Digital Certification Agency

PKI Disclosure Statement Of TnTrust Corporate CA

Review

Rev	Date	Comment	Page
00	15/02/2017	1 st version	All pages

	Author	Verified by	Approved by
Entity :	NDCA	Board Committee	CEO
Date :	10/08/2016	15/02/2017	15/02/2017



	POLICY	Code : PL/TC/11 Rev : 00
	PKI Disclosure Statement of TnTrust Corporate CA	Date : 15/02/2017 Page : 2/7 NC: PU

Table of Contents

1. Notice	3
2. Contact Information	3
3. Certificate type, Validation procedures and Usage	3
4. Reliance limits	4
5. Obligations of subscribers	4
6. Certificate status checking obligations of relying parties	5
7. Limited warranty and disclaimer/Limitation of liability	5
8. Applicable agreements, CPS and CP	6
9. Privacy Policy	7
10. Refund Policy	7
11. Applicable law, complaints and dispute resolution	7
12. CA and Repository licenses, trust marks and audit	7

	POLICY	Code : PL/TC/11 Rev : 00
	PKI Disclosure Statement of TnTrust Corporate CA	Date : 15/02/2017 Page : 3/7 NC: PU

1. Notice

This document is the PKI Disclosure Statement, hereinafter referred to as the PDS, of the TN PKI CA of the National Digital Certification Agency in Tunisia (referred to as NDCA). This document does not substitute or replace the Certificate Policy nor the Certification Practice Statement (CP/CPS) under which digital certificates of the NDCA are issued.

This statement, which follows the structure of Annex A of the document ETSI TS 411 319-1, is merely informative and in no way replaces the provisions of the aforementioned documents.

2. Contact Information

Queries regarding this PKI Disclosure Statement shall be addressed to:

The National Digital Certification Agency,
Address: Technopark El Ghazala, Road of Raoued Km 3.5 , Ariana 2083 - Tunisia
E-mail: ndca.pki@certification.tn
Tel : +216 70 834 600
Fax : +216 70 834 555
Website: www.certification.tn

3. Certificate type, Validation procedures and Usage


Certificate Type

This statement applies only to qualified certification services provided by NDCA. Public key qualified certificates are issued by the qualified certification authority “TnTrust Qualified Corporate CA”. Profile and any other limitation of certified public key certificate issued by the “TnTrust Qualified Corporate CA” is compliant with the ETSI EN 319 411-2.

Validation procedure

Qualified certificate is issued to an individual after verification of their identity. Verification of the individual may be carried out by a registration authority or other person who is authorized to confirm identity of the certificate holder. The individual, requesting issuance of a qualified certificate shall be identified by his national identity document. In case of individuals associated or acting on behalf of an organization, the authorization of the subscriber (the signatory) to act and to use the certificate on behalf of the organization is required or the official government or trade register record of the powers is required.

The identification and authentication of an applicant for a certificate must meet the requirements specified in Section 3.2 (Initial Identity Validation) of the CP/CPS. The CA or RA shall identify and authenticate all required subscriber information in terms of Section 3.2 (Initial Identity Validation) of the aforementioned CP/CPS.

	POLICY	Code : PL/TC/11 Rev : 00
	PKI Disclosure Statement of TnTrust Corporate CA	Date : 15/02/2017 Page : 4/7 NC: PU

Usage

Qualified certificates issued by TnTrust Qualified Corporate CA may be used only in accordance with EN ETSI TS 319 411-2.

4. Reliance limits


The TnTrust Qualified Corporate 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 NDCA system and supervise NDCA users and personnel efficiently, all events occurring in the system and having essential impact on NDCA 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

Subscribers are required to act in accordance with the CP/CPS and the relevant Subscriber Agreement. In this context, Subscribers are responsible for:

- 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 registration form;
- supplementing such information with a proof of identity and the provision of the information;
- 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 this CP/CPS and other relevant regulations and agreements;
- ensuring complete control over the private key by not sharing private keys and / or passwords;
- notifying the registration authority 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 the registration authority 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

	POLICY	Code : PL/TC/11 Rev : 00
	PKI Disclosure Statement of TnTrust Corporate CA	Date : 15/02/2017 Page : 5/7 NC: PU

(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;
- protecting the private key from unauthorized access.

In addition to that, for Qualified Certificates, private keys are generated on a Secure Signature Creation Device (SSCD) with the presence of the subscriber who is the one responsible for securing the SSCD.

6. Certificate status checking obligations of relying parties

Relying parties are allowed to use certificates only in accordance with the terms and conditions set forth in the CP/CPS. It is in their sole responsibility to verify legal validity and applicable policies.

To verify the validity of a digital certificate they received, relying parties must refer to the CRL or OCSP response prior to relying on information featured in a certificate to ensure that the TnTrust Qualified Corporate CA has not revoked the certificate. The locations of the CRL distribution point and OCSP responder are detailed within the certificate.


A relying party is committed to:

- verify that an electronic signature has been created by means of a private key corresponding to a public key set in the subscriber's certificate issued by NDCA,
- verify that a signed message/document or a certificate have not been modified after signing it,
- carry out cryptographic operations accurately and correctly, using the software and devices whose security level complies with the sensitivity level of the certificate being processed and the trust level of applied certificates,
- consider the electronic signature or the certificate to be invalid if by means of applied software and devices it is not possible to state if the electronic signature or the certificate are valid or if the verification result is negative;
- trust only these qualified certificates that are used in accordance with the declared purpose and are appropriate for applicability ranges that were specified by the relying party, and the status was verified on the basis of the valid Certificate Revocation Lists or OCSP service available at NDCA.

7. Limited warranty and disclaimer/Limitation of liability

The TnTrust Qualified Corporate CA warrants and promises to:

- Provide certificates issuance and repository services consistent with the CP/ CPS and other NDCA Operations Policies and Procedures.

	POLICY	Code : PL/TC/11 Rev : 00
	PKI Disclosure Statement of TnTrust Corporate CA	Date : 15/02/2017 Page : 6/7 NC: PU

- At the time of Certificate issuance, TnTrust Qualified Corporate CA implement procedure for verifying accuracy of the information contained within it before installation and first use,
- Implement a procedure for reducing the likelihood that the information contained in the Certificate is not misleading,
- Maintain 24 x 7 publicly-accessible repositories with current information,
- Perform authentication and identification procedures in accordance with the CP/CPS and the internal Operations Policies and Procedures,
- Provide certificate and key management services including certificate issuance, publication and revocation in accordance with the TnTrust Qualified Corporate CA CP/CPS,
- Subscribers or Relying Parties for making no direct warranties or promises.

The TnTrust Qualified Corporate CA does not liable for any loss of the PKI service:

- Due to war, natural disasters, etc.
- Due to unauthorized use of certificates or using it beyond the prescribed use defined by the TnTrust Qualified Corporate CP/CPS for the certificates issued by the TnTrust Qualified Corporate CA.


Limitations on Liability:

- The TnTrust Qualified Corporate CA will not incur any liability to Subscribers or any person to the extent that such liability results from their negligence, fraud or willful misconduct.
- The TnTrust Qualified Corporate CA assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under Certificate Policy for any use other than in accordance with Certificate Policy. Subscribers will immediately indemnify the TnTrust Qualified Corporate CA from and against any such liability and costs and claims arising there from.
- The TnTrust Qualified Corporate CA will not be liable to any party whatsoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services.
- End-Users are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by TnTrust Qualified Corporate CA.
- Subscribers to compensate a Relying Party which incurs a loss as a result of the Subscribers breach of Subscriber's agreement.
- TnTrust Qualified Corporate CA denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation.

8. Applicable agreements, CPS and CP

The TnTrust Qualified Corporate CA CP/CPS can be found on the website of the NDCA at <http://www.certification.tn/pub/CPCPS-TunisianNationalPKI.pdf>.

As for the Subscriber Agreement and the Relying Party Agreement, they may be found on the website of the NDCA at <http://www.certification.tn>.

	POLICY	Code : PL/TC/11 Rev : 00
	PKI Disclosure Statement of TnTrust Corporate CA	Date : 15/02/2017 Page : 7/7 NC: PU

9. Privacy Policy

NDCA fully complies with the Tunisian Act on the protection of personal data and other applicable legislation in Tunisia.

Any information about subscribers that is not made public through the certificates issued by the TnTrust Qualified Corporate CA or the CRL is considered private information. Any and all information made public in a certificate issued by TnTrust Qualified Corporate CA, or its CRL, or by a publicly available service shall not be considered confidential.

NDCA retain all events relating to the life cycle of keys managed by the CA for at least seven years after any certificate based on these records ceases to be valid.

10. Refund Policy

Currently, no fees are charged by TnTrust Qualified Corporate CA for Digital Certificates, although TnTrust Qualified Corporate CA reserves the right to change this in the future. Digital Certificates for which no charge is made, no refunds are possible. In addition a Corporate CSP may charge fees for its service.

11. Applicable law, complaints and dispute resolution

Certificates issued by the TnTrust Qualified Corporate CA, the CP/CPS, Subscriber Agreement is governed by the laws and regulations of Tunisia.

In case of any dispute or controversy between parties including NDCA partners, Subscribers and Relying Parties, shall be submitted 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 Corporate 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 Tunisian National 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.