National Digital Certification Agency

CP / CPS of the Tunisian National PKI

Review

Rev	Date	Comment	Page
00	15/02/2017	1st Writing	Whole document
01	17/03/2017	1st revision	Section 1.1, 4.93, 4.12.1, 5.2.1, 6.2.3, 7.1
02	21/04/2017	2nd revision	Sections 1.1, 4.9.8, 7.1.2.1, 7.1.2.2, 7.4
03	27/11/2017	3rd revision	Sections 1.3.7

	Author	Verified by	Approuved by
Entity :	NDCA	Board Commitee	CEO
Date :	24/09/2017	22/11/2017	27/11/2017

Table of Contents

1 INTRODUCTION

The « Tunisian National Root CA » is a root certification authority operated by the National Digital Certification Agency.

The « Tunisian National Root CA » only issues certificates to its subordinated intermediate CAs and special purpose certificates for the operation of the Certificate Service Provider.

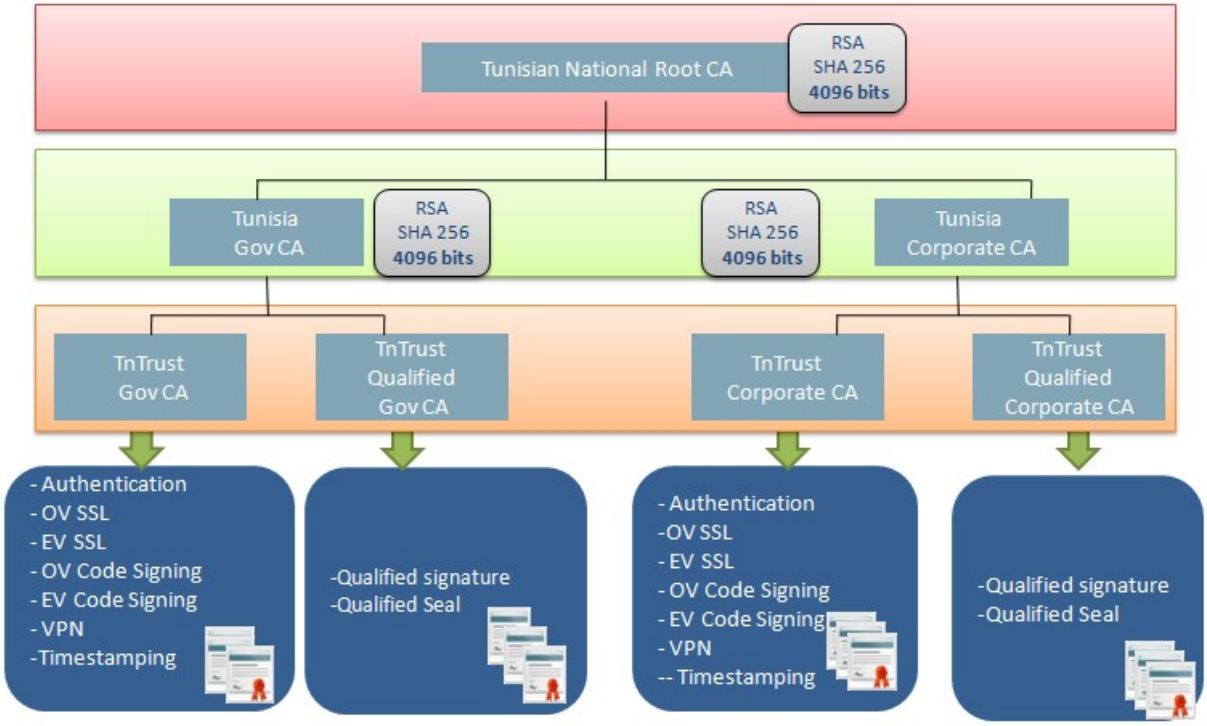
This CP/CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. The certification authorities within the Tunisian National Root CA conform to the current version of the CA/Browser Forum (CABF) requirements including:

- Guidelines for the Issuance and Management of Extended Validation (EV) Certificates,
- Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates, and,
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,

Published at www.cabforum.org. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document.

1.1 Overview

The picture below shows the structure of the « Tunisian National Root CA » tree:



This certificate policy and certification practice statement (CP/CPS) for the « Tunisian National Root CA » and all its subsidiaries CAs describes:

- The certification and registration policy of this CA.
- Practices and procedures of this CA.
- Practices and procedures of the registration authorities for this CA.
- Terms and conditions under which this CA is made available.

This CP/CPS is applicable to all persons, including, without limitation, all requesters, subscribers, relying parties, registration authorities and any other persons, that have a relationship with the National Digital Certification Agency with respect to certificates issued by a subsidiary CA of the "Tunisian National Root CA".

This CP/CPS also provides statements of the rights and obligations of the TN PKI's CAs, authorized registration authorities, requesters, subscribers, relying parties, resellers, co-marketers and any other person, or organization that use or rely on certificates issued by a subsidiary CA of the "Tunisian National Root CA".

The OID of NDCA (ANCE) is : joint-iso-itu-t(2) country(16) tn(788) public-sector(1) public-sector-entreprises(2) ance(6).

The SubCAs "TnTrust Gov CA" and "TnTrust Corporate CA" are under Policy OID : 2.16.788.1.2.6.1.9.
The SubCAs "TnTrust Qualified Gov CA" and "TnTrust Qualified Corporate CA" are under Policy OID : 2.16.788.1.2.6.1.10.

TN PKI CA issues certificates containing the following OID arcs:

a) End User Certificates issued by TnTrust Gov CA:

Service	Description	OID
Organisation Validation SSL	A Certificate to authenticate servers	OVCP OID: 0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.1.1
Wildcard SSL	A Certificate to authenticate servers .Secure SSL certificates that secure multiple hosts on a single domain on the same server.	OVCP OID: 0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.1.1
Extended Validation SSL	A Certificate to authenticate servers. Extended validation secure SSL certificates issued by TN PKI in conformance with the Guidelines for Extended Validation Certificates.	EVCP OID: 0.4.0.2042.1.4 OID: 2.16.788.1.2.6.1.9.1.2
Code Signing	A Certificate to authenticate data objects	OVCP OID:0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.1.3
Extended Validation Code Signing	A Certificate to authenticate data objects	EVCP OID: 0..4.0.2042.1.4 OID: 2.16.788.1.2.6.1.9.1.4
Authentication	A Certificate to authenticate person	NCP+ OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.9.1.5
Qualified Digital Signature	A Certificate to issue an electronic signature that is compliant to EU Regulation No 910/2014 (e-IDAS Regulation) for electronic transactions within the internal European market.	NCP+ OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.1
TimeStamping	A Certificate to issue timestamp tokens	NCP+ OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.9.1.7
VPN	A Certificate to encrypt transactions between gateways.	OVCP OID: 0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.1.6

b) End User Certificates issued by TnTrust Corporate CA:

Certificate Type	Description	OID
Organisation Validation SSL	A Certificate to authenticate servers	OVCP OID: 0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.2.1
Wildcard SSL	A Certificate to authenticate servers	OVCP

	.Secure SSL certificates that secure multiple hosts on a single domain on the same server.	OID: 0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.2.1
Extended Validation SSL	A Certificate to authenticate servers. Extended validation secure SSL certificates issued by TN PKI in conformance with the Guidelines for Extended Validation Certificates.	EVCP OID: 0.4.0.2042.1.4 OID: 2.16.788.1.2.6.1.9.2.2
Code Signing	A Certificate to authenticate data objects	OVCP OID:0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.2.3
Extended Validation Code Signing	A Certificate to authenticate data objects	EVCP OID: 0..4.0.2042.1.4 OID: 2.16.788.1.2.6.1.9.2.4
Authentication	A Certificate to authenticate person	NCP+ OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.9.2.5
VPN	A Certificate to encrypt transactions between gateways.	OVCP OID: 0.4.0.2042.1.7 PID: 2.16.788.1.2.6.1.9.2.6

c) End User Certificates issued by TnTrust Qualified Gov CA:

Service	Description	OID
Qualified Digital Signature	A Certificate to issue an electronic signature that is compliant to EU Regulation No 910/2014 (e-IDAS Regulation) for electronic transactions within the internal European market.	NCP+ OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.1
Qualified Seal	Qualified certificates for electronic seal (eSeal) are intended for the creation of qualified electronic seals in accordance with law no. 272/2016 Coll and EU Regulation no. 910/2014 eIDAS. Qualified certificates for eSeal are issued to legal persons or public authorities, always on the hardware device.	NCP+ OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.2

d) End User Certificates issued by TnTrust Qualified Corporate CA:

Service	Description	OID
Qualified Digital Signature	A Certificate to issue an electronic signature that is compliant to EU Regulation No 910/2014 (e-IDAS Regulation) for electronic transactions within the internal European market.	NCP+ OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.2.1
Qualified Seal	Qualified certificates for electronic seal	NCP+

	(eSeal) are intended for the creation of qualified electronic seals in accordance with law no. 272/2016 Coll and EU Regulation no. 910/2014 eIDAS. Qualified certificates for eSeal are issued to legal persons or public authorities, always on the hardware device.	OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.2.2

For the issuance of Extended Validation SSL certificates, the National Digital Certification Agency fully complies with all the rules and regulations published by the CA/Browser Forum (http://www.cabforum.org/):

- EV Guidelines: "Guidelines for the Issuance and Management of Extended Validation Certificates".

For the issuance of qualified certificates the National Digital Certification Agency fully complies with all the rules and regulations published by:

- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI) – Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI TS 101 861: Time Stamping Profile
- IETF RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework
- IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

1.2 Document Name and identification

This CP/CPS, named « CP/CPS of the Tunisian National PKI», is the property of the National Digital Certification Agency.

The version number and date of the document is provided herein on the cover page.

TN PKI CP/CPS document describes how NDCA conducts its activities relating to certification services.

This CP/CPS document is disclosed to the public at the website http://www.certification.tn.

The OID of the present document is: 2.16.788.1.2.6.1.9.

1.3 PKI Participants

1.3.1 Certification Authority (CA)

1.3.1.1 Root certification authority

The Tunisian National root CA is the primary trust point for the entire PKI architecture.
The « Tunisian National Root CA» and its subsidiary CAs are the only public CAs operated by the National Digital Certification Agency that issue certificates under this CP/CPS.

The obligations of Root CA are:

- Operate and manage the Root CA system and its functions;
- Issue and manage certificates for designated Government or Accredited Private CAs (Subordinate CAs);
- Re-key of the Root CA and approved CA signing keys;
- Establishment and maintenance of the CPS;
- Support international cooperation on certification service, including mutual recognition and cross-certification; and
- Notification of issuance, revocation or renewal of its certificates.

The TN PKI Root CA servers are not reachable through the network.

1.3.1.2 Subordinate Certification Authorities

The « Tunisian National Root CA » has two intermediate CAs:

- The « Tunisia GOV CA »: This SubCA is expected to perform the issuance of the issuing Certification authorities of TnTrust in the level 3 of hierarchy:
  - TnTrust GOV CA : this CA issue certificates for :
    - devices : SSL certificates such as OV (Organization Validation), Standard SSL and multi-domain SSL, VPN certificate, code signing certificate, OCSP certificate, Timestamp authority certificate, …
    - natural and legal persons: authentication certificate, signature certificate, certificate for mobile, organization certificate…

    This CA concerns only certificates for governmental organizations.
  - TnTrust Qualified GOV CA: this CA issue certificates for :
    - devices : EV SSL certificates, EV Code signing
    - natural and legal persons: Qualified digital signature certificate…

    This CA concerns only certificates for governmental organizations.

- The « Tunisia Corporate CA »: This SubCA is expected to perform the issuance of the issuing Certification authorities of TnTrust in the level 3 of hierarchy:
  - TnTrust Corporate CA : this CA issue certificates for :
    - devices : SSL certificates such as OV (Organization Validation), Standard SSL and multi-domain SSL, VPN certificate, code signing certificate, OCSP certificate, Timestamp authority certificate, …
    - natural and legal persons: authentication certificate, signature certificate, certificate for mobile, organization certificate…

    This CA concerns only certificates for corporate organizations.
  - TnTrust Qualified Corporate CA: this CA issue certificates for :
    - devices : EV SSL certificates, EV Code signing
    - natural and legal persons: Qualified digital signature certificate…

    This CA concerns only certificates for corporate organizations.

The intermediate CA servers are not reachable through the network.
The issuing CA servers are kept online.

The obligations of the Subordinate CAs are:

- Operate and manage the subordinate CA system and its functions in accordance with this CP/CPS;
- Issue and manage certificates for Issuing CAs; and
- Notification of issuance, revocation or renewal of its certificates.

The obligations of Issuing CAs are:

- Operate and manage the Issuing CA system and its functions in accordance with this CP/CPS;
- Issue and manage certificates to user or juridical entities, used for general or specific purpose;
- Publish issued certificates and revocation information;
- Handle revocation request regarding certificate issued by the TN PKI CAs; and
- Notification of issuance, revocation or renewal of its certificates.

1.3.2 Registration Authority (RA)

The National Digital Certification Agency operates a registration authority, called TN PKI RA that registers subscribers of certificates issued by the subsidiary CAs of the “Tunisian National Root CA”.
The TN PKI RA performs certain functions pursuant to an RA Agreement including the following:

- Identify the user and register the user information;

- Transmit certificate request to the TN PKI CA;
- Validate certificates from the TN PKI CA Directory Server and CRL, and if available, via Online Certificate Status Protocol (OCSP);
- Prepares, and provides or makes available secure cryptographic devices, or other secure devices, to subscribers; and
- Request revocation of certificates.

1.3.3 Delegated Registration Authority (DRA)

Delegated RAs have to abide by all the requirements of the TN PKI CP/CPS. DRAs may, however implement more restrictive practices based on their internal requirements.

Any DRA operating under this CP/CPS must adhere to the following rules:

• The DRA must have a contractual agreement with the National Digital Certification Agency which indicates the authorization for their role as RA and clearly details the minimum requirements, processes and liabilities.

• The registration process of any DRA must be provided by the National Digital Certification Agency. The latter has to audit and approve the process as meeting the quality requirements of this CP/CPS and therefore being equivalent to the registration process of the TN PKI RA.

• The DRA must have an annual audit. All costs related to this audit are to be paid by the operator of the RA. Failure to pass the annual audit leads to the revocation of DRA privileges.

1.3.4 Subscriber and subject

The subject can be:

- A natural person,
- A natural person identified in association with a legal person,
- A legal person (that can be an organization or a department identified in association with an organization), or
- A device or system operated by or on behalf of a natural or legal person.

This CP/CPS specifies two types of subscribers :

- The subscriber is the subject
- The subscriber is acting on behalf of one or more distinct subjects to whom it is linked (e.g. the subscriber is a organization requiring certificates for its employees to allow them to participate in electronic business on behalf of the company),

In the context of this CP/CPS, subscribers include all end users of certificates issued by the issuing CAs under the Tunisian National Root CA. A subscriber is the entity named as the end-user Subscriber of a certificate.
The link between the subscriber and the subject is one of the following:

- To request a certificate for natural person the subscriber is:
    - the natural person itself;
    - a natural person mandated to represent the subject; or
    - any entity as allowed under the relevant legal system to represent the legal person for which the person is identified in association with the "Organization" field of the certificate (such as the company employing the natural person or a non-profit legal person the natural person is member of).
- To request a certificate for legal person the subscriber is:
    - any entity as allowed under the relevant legal system to represent the legal person, or
    - a legal representative of a legal person subscribing for its subsidiaries or units or departments.
- To request a certificate for a device or system operated by or on behalf of a natural or legal person the subscriber is:
    - the natural or legal person operating the device or system;
    - any entity as allowed under the relevant legal system to represent the legal person; or
    - a legal representative of a legal person subscribing for its subsidiaries or units or departments.

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 as specified in section 3;
- 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 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 (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.

1.3.5 Relying party

Relying parties are individuals or organizations that use certificates of any subsidiary CA of the "Tunisian National Root CA" to validate the signatures and verify the identity of subscribers and/or to secure communication with these subscribers. Relying parties are allowed to use such certificates only in accordance with the terms and conditions set forth in this 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 issuing CA under the Tunisian National Root CA has not revoked the certificate. The locations of the CRL distribution point and OCSP responder are detailed within the certificate.

1.3.6 Representative of subscriber

Representative of subscriber is a natural person directly by law, by Delegation or by proxy of the subscriber, have the power to carry out a request for the certificate 's issuance and the execution of the subscriber Certificate Agreement.

1.3.7 Board committee

The Board committee in NDCA is composed of persons directly attached to the general management department. This committee is chaired by the CEO of NDCA.

Typical duties of this committee include:

- Governing the organization by establishing board policies and setting out strategic objectives;
- Management commitment

- Resource allocation
- Validation of information security management policies and procedures as well as security objectives, including this Policy
- Acceptance of residual risks and validation of the risk management plan

1.3.8 Other participants

Other participants are individuals or organizations that rely on the certificate of a subscriber, or are in some way involved with certificate manufacturing and may or may not wish to verify the identity of subscribers and/or to secure communication with this subscriber.
Other participants can be also subscribers within this CA.

1.4 Certificate Usage

1.4.1 Appropriate certificate usage

1.4.1.1 Certificate of the CA

The Tunisian National Root CA private key is used to sign certificates in the following cases:

- Self-signed certificates to represent the Root CA itself;
- Certificates for intermediate CAs;
- Certificates for infrastructure purposes (e.g. OCSP Response verification Certificates).

1.4.1.2 Certificates of the intermediate CAs

The Tunisia GOV CA and the Tunisia Corporate CA certificates are issued by the Tunisian National Root CA with the following key usage bits set: digitalSignature, Key CertSign and CRL Sign.
The intermediate CAs certificates can only be used for signing certificates, CRLs, OCSP and time stamp certificates, as well as for verification of subject certificates and data.

1.4.1.3 Certificates of the issuing CAs

The issuing CAs are issued with the following key usage bits set: digitalSignature, Key CertSign and CRL Sign.

.

Certificates issued by TN PKI Issuing CAs can only be used strictly as part of the framework of the limitations incorporated in the certificates:

a) Certificates Issued to Individuals

Individual Certificates are normally used by individuals to sign e-mail and to authenticate to applications (client authentication). The most common usages for individual certificates are: Signing and Client Authentication.

b) Certificates Issued to Organizations

Organizational Certificates are issued to organizations after authentication that the Organization legally exists and that other Organization attributes included in the certificate (excluding non-verified subscriber information) are authenticated e.g. ownership of an Internet or e-mail domain. The most common usages are: Code/ Content Signing, Secure SSL/TLS- sessions, Authentication and Signing.

1.4.2 Prohibited Certificate Uses

All issued certificates under this CP/CPS cannot be used for purposes other than what is allowed in Section 1.4.1 (Appropriate Certificate Usage) above.

1.5 Policy Administration

1.5.1 Organization administering the document

The Tunisian National Root CA CP/CPS is written and updated by the National Digital Certification Agency.

National Digital Certification Agency

Technopark El Ghazala,

Road of Raoued,

Ariana, 2083

Tunisia.

Tel.: +216 70 834 600

Mail: ance@certification.tn

Web: http://www.certification.tn

Current versions of documents are downloaded from the NDCA website:

http://www.certification.tn

1.5.2 Contact person

The following person is the main contact for any questions or suggestions regarding the Tunisian National Root CA:

PKI Policy Manager, ndca.pki@certification.tn

All feedback, positive or negative, is welcome and should be submitted to the above e-mail address to ensure that it is dealt with appropriately and in due time.

1.5.3 Person determining CPS suitability for the policy

The Board Committee of the National Digital Certification Agency determines the suitability and applicability of this CP/CPS.

1.5.4 CP/CPS approval procedures

This CP/CPS is approved by the board committee along with the CEO. After being approved, the National Digital Certification Agency will publish it on its website.

The updated version is binding upon all Subscribers including the Subscribers and parties relying on Certificates that have been issued under a previous version of the CPS.

1.6 Definitions and Acronyms

Term	**Abbrev.**	**Explanation**
Algorithm		A process for completing a task. An encryption algorithm is merely the process, usually mathematical, to encrypt and decrypt messages.
Attribute		Information bound to an entity that specifies a characteristic of that entity, such as a group membership or a role, or other information associated with that entity.
Authentication		The process of identifying a user. User names and passwords are the most commonly used methods of authentication.

CA Operator	CAO	A person responsible for CA operation, including establishment of certificate parameters for RA and RAO in accordance with certificate policy.
Certificate		Information issued by a trusted third party, often published in a directory with public access. The certificate contains at least a subject, a unique serial number, an issuer and a validity period.
Certification Authority	CA	An internal entity or trusted third party that issues, signs, revokes, and manages digital certificates.
Certificate Extension		Optional fields in a certificate.
Certificate Policy	CP	A set of rules that a request must comply with in order for the RA to approve the request or a CA to issue the certificate.
Certificate Revocation List	CRL	List of certificates that have been declared invalid. This list is issued by the CA at regular intervals and is used by applications to verify the validity of a certificate.
Certification Practice Statement	CPS	Document that regulates the rights and responsibilities of all involved parties (RA, CA, directory service, end entity, relying party).
Certification Service Provider	CSP	Individual or corporation that issues certificates to individual or corporate third parties.
Cipher		A cryptographic algorithm used to encrypt and decrypt files and messages.
Cipher Text		Data that has been encrypted. Cipher text is unreadable unless it is converted into plain text (decrypted) with a key.
Coordinated Universal Time	UTC	Mean solar time at the prime meridian (0°).
Credentials		Evidence or testimonials governing the user's right to access certain systems (e.g. User name, password, etc)
Decryption		The process of transforming cipher text into readable plain text.
Digital signature		A system allowing individuals and organizations to electronically certify features such as their identity or the

Distinguished Name	DN	→ Subject
DNS		Domain Name System. The Internet system of holding a distributed register of entity names.
Electronic Signature		→ Digital Signature
Encryption		Encryption is the process of using a formula, called an encryption algorithm, to transform plain text into an incomprehensible cipher text for transmission.
End Entity		Used to describe all end users of certificates, i.e. subscribers and relying parties.
End-User Agreement	EUA	Contractual agreement between seller of certificates and the subscriber.
Enterprise EV Certificate		An EV certificate that an enterprise RA authorizes the CA to issue at third and higher domain levels that are contained within the domain that was included in an original valid EV certificate issued to the enterprise RA.
Entropy		A numerical measure of the uncertainty of an outcome. The entropy of a system is related to the amount of information it
EV Certificate		A digital certificate that contains information specific in the EV guidelines and that has been validated in accordance with the guidelines.
Extended Validation	EV	Validation procedures defined by the guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and major browser vendors.
Extension		→ Certificate Extension
FIPS 140		FIPS 140 (Federal Information Processing Standards Publication 140) is a United States federal standard that specifies security requirements for cryptography modules.
FQDN	FQDN	Fully Qualified Domain Name.
Hardware Security Module	HSM	Hardware Security Module is a device that physically protects key material against unauthorized parties.

HTTP	HTTP	Hyper-Text Transfer Protocol used by the Internet. HTTP defines how data is retrieved or transmitted via the Internet and what actions should be taken by web servers and browsers.
HTTPS	HTTPS	Secure Hyper-Text Transfer Protocol using TLS/SSL
Key		The secret input for cryptographic algorithms that allows a message to be transformed. → See Private Key, Public Key
Key password		Password used to encrypt the private key.
Key size		Length of private and public key.
Key usage		Key's intended purpose. This information is stored in the certificate itself to allow an application to verify that the key is intended for the specified use.
Lightweight Directory Access	LDAP	LDAP is used to retrieve data from a public directory.
LDAP Secure	LDAPS	LDAP secured with TLS/SSL
National Digital Certification Agency	NDCA	
Online Certificate Status Protocol	OCSP	Method to verify the validity of a certificate in real time.
Participants		Entities like CAs, RAs, and repositories. These can be different legal entities.
PKCS		PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA Laboratories.
Plain Text		The original message or file.
Private Key		One of two keys used in public key cryptography. The private key is known only to the owner and is used to sign outgoing messages or decrypt incoming messages.

Public Key		One of two keys used in public key cryptography. The public key can be known to anyone and is used to verify signatures or encrypt messages. The public key of a public-private key cryptography system is used to verify the “signatures“ on incoming messages or to encrypt a file or message so that only the holder of the private key can decrypt the file or message.
Public Key Infrastructure	PKI	Processes and technologies that are used to issue and manage digital identities that are used by third parties to authenticate individuals or organizations.
RA Operator	RAO	The person responsible for identifying the requester, collecting the identity substantiating evidence, authorizing the CSR, and forwarding the authorized CSR to the CA.
Relying Party		Recipient of a certificate which acts in reliance on that certificate and/or digital signatures verified using that certificate.
Revocation		Invalidation of a certificate. Every CA regularly issues a list of revoked certificates called CRL. This list should be verified by all applications using certificates from that CA before trusting a certificate.
RSA		A public key encryption algorithm named after its founders: Rivest-Shamir- Adleman.
S/MIME		Secure / Multipurpose Internet Mail Extensions is a standard for public key encryption and signing of e-mail.
Secure Signature Creation Device	SSCD	Signature-creation device which meets the requirements specified in annex III of Directive 1999/93/EC.
Smart-card		Credit Card or SIM-shaped carrier of a secure crypto processor with tamper- resistant properties intended for the secure storage and usage of private keys.
Signature		Cryptographic element that is used to identify the originator of the document and to verify the integrity of the document.
Signature-creation data		Unique data, such as parameters of signature algorithms or private cryptographic keys, used by the signatory to create an electronic signature.

Signature-creation device		Configured software or hardware used to implement the signature-creation data
Signature-verification data		Data, such as parameters of signature algorithms or public cryptographic keys, used for the purpose of verifying an electronic signature.
SSL/TLS		Secure Sockets Layer. A protocol developed by Netscape that enables secure transactions via the Internet. URLs that require an SSL/TLS connection for HTTP start with https: instead of http:.
SSO		Single Sign On: The user only needs to log in once to access various services.
Subject	DN	Field in the certificate that identifies the owner of the certificate. Also referred to as distinguished name (DN).
Subscriber		Subscribers are individuals that have obtained a certificate.

2 Publication and Repository Responsabilities

2.1 Repositories

The National Digital Certification Agency publishes this CP/CPS, certificate terms and conditions, the relying party agreement and the subscriber agreement in its official web site at http://www.certification.tn.
Any revocation data on issued digital certificates is published at location of the CRL distribution point or OCSP responder specified in the certificate (http://va.certification.tn).

2.2 Publication of Certification Informations

TN PKI publishes all current documentation pertaining to the Tunisian National Root CA and its subsidiaries on the certification.tn web site. This web site is the only source for up-to-date documentation and TN PKI reserves the right to publish newer versions of the documentation without prior notice.

For the Tunisian National Root CA and its subsidiaries, TN PKI will publish an approved and current version of:

- the certificate policy and certification practice statement (CP/CPS)
- the end-user agreement (EUA)
- the pricing information

TN PKI publishes information related to certificates issued by this CA on the certification.tn web site. The certification.tn web site and the LDAP directory ldap://ldap.certification.tn are the only authoritative sources for:

- All publicly accessible certificates issued by the TN PKI CAs.
- The certificate revocation list (CRL) for the TN PKI CAs. The CRL is downloaded from the crl.certification.tn web site. The exact URL is documented in every certificate that is issued by one of the subsidiaries of the Tunisian National Root CA in the field: “CRL Distribution Point“. Meanwhile, subscriber or relying party can get the current state of certificate instantly via OCSP service (va.certification.tn) provided by the TN PKI.
- The data formats used for certificates issued by the subsidiaries of the Tunisian National Root CA and for certificate revocation lists in the certification.tn web site are in accordance with the associated schema definitions as defined in the X.500 series of recommendations.

Certificate dissemination services are available 24 hours per day, 7 days per week.

2.3 Time or Frequency of Publication

The National Digital Certification Agency will publish these informations on a regular schedule:

- CRLs for the Tunisian National Root CA and all its subsidiaries are published according to the schedule detailed in section 4.9.7.
- OCSP Information: The OCSP responder will immediately report a certificate that has been revoked.

The National Digital Certification Agency will publish the most current version and all superseded versions of the following publications on its web site:
This CP/CPS will be reviewed at least once a year. If no updates are required, no new version will be published.

2.4 Access controls on repositories

The information in the National Digital Certification Agency repository is publicly available. Read-only access to such information is unrestricted.
With network security, the National Digital Certification Agency ensures that only authorized employees can add, delete, modify and publish the repositories.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

The distinguished name (DN) in a certificate issued by the Tunisian National Root CA or one of its subsidiaries complies with the X.500 standard.

For the distinguished name, a minimum of one field is required. This field is /CN=. For the common name (CN), the National Digital Certification Agency allows several types of names to be specified:

- Real names : Real names are specified as /CN='First Name' 'Last Name' or /CN='Organizational Name'.
  First, Middle and Last Name in the CN have to be absolutely identical to the names as they appear in the identifying documentation provided.
- Organization names: The organizational name in /CN or in /O is spelled absolutely identical to the name as it appears in the documentation provided according to the section 3.2.2.

  If the CN is an organizational name, then the entries in the /O and /C field are also inserted. In this case the /CN field is identical to the /O field.
- Fully qualified domain names (FQDN): FQDNs is well formed according to RFC 1035.
- SubjectAltName is a recommended field for certificates issued with real name. If it is present, it contains at least an FQDN.

Additional attributes in the SubjectAltName are permissible in any certificate and may be supported by the RA at their own discretion:

otherName	content to be verified by the RA
rfc822Name	e-mail address according to rfc 5322
dNSName	FQDN, fully qualified domain name according to rfc 1035.
x400Address	content to be verified by the RA.
directoryName	content to be verified by the RA.
ediPartyName	content to be verified by the RA.

uniformResourceIdentifier	URI according to rfc 3986.
registeredID	OID, content to be verified by the RA.

3.1.2 Need for names to be meaningful

The subject and issuer name contained in a certificate are meaningful in the sense that the RA has proper evidence of the existent association between these names and the entities to which they belong.

3.1.3 Anonymity or pseudonymity of subscribers

The National Digital Certification Agency does not issue anonymous or pseudonymous certificates.

3.1.4 Rules for interpreting various name forms

Many languages have special characters that are not supported by the ASCII character set used to define the subject in the certificate. To avoid problems, local substitution rules are used in general, national characters are represented by their ASCII equivalent, e.g. é, è, à, ç are represented by e, e, a, c.

3.1.5 Uniqueness of names

The CAs operating under this CP/CPS enforce the uniqueness of certificate subject fields in such a manner that all valid certificates with identical subject fields belong to the same individual or organization.

3.1.6 Recognition, authentication, and role of trademarks

Subject's DN of certificate issued by a subsidiary of the Tunisian National Root CA does not contain trademark.

3.2 Initial Identity Validation

The TN PKI RAs verify the identity of the subscriber and subject and check that certificate requests are accurate, authorized and complete according to the collected evidence or attestation of identity.

The initial identity validation is part of the Certificate Application Process as described in section 4.1.

3.2.1 Method to prove possession of private key

3.2.1.1 Certificates for devices

The subscriber provides a digitally signed PKCS#10 CSR to establish that it holds the private key corresponding to the public key to be included in a certificate. TN PKI RA parses the PKCS#10 CSR submitted by the subscriber and verifies that the subscriber's digital signature on the PKCS#10 was created by the private key corresponding to the public key in the PKCS#10 CSR.

3.2.1.2 Certificates for persons

In this case, the private key generation is under the TN PKI CA or RA's direct control (in a secure cryptographic device). So the proof of possession is no longer required.

3.2.2 Authentication of organization identity

The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to:

- The use of the organization field means that the use of the country field is mandatory.
- The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name.
- To validate the name of the organization, the requester provides official documentation about the organization.
- The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form.
- The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation.
  Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form.

3.2.2.1 CABF Verification Requirements for Organization Applicants

EV SSL Certificates, EV Code Signing, and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the TN PKI Supplemental Procedures, Appendix A, Appendix B and Appendix C, respectively.

3.2.2.2 Mozilla Verification Requirements for Organization Applicants

For requests for internationalized domain names (IDNs) in Certificates, the Tunisian National Root CA performs domain name owner verification to detect cases of homographic spoofing of IDNs. It employs a manual process that searches various 'whois' services to find the owner of a particular domain. A search failure result is flagged for manual review and the RA may manually reject the Certificate Request. Additionally, the RA rejects any domain name that visually appears to be made up of multiple scripts within one hostname label.

3.2.3 Authentication of individual identity

Various individuals may need to authorize the use of names in different parts of the DN. The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of such individuals. The regulations defined in the registration forms may be summarized as follows:

- The registration form carry original, personal handwritten signatures.
- The wording in the request has to be identical to the given name(s) and the family name of the identifying documents.

Additionally, the requester and only the requester is identified according to these additional rules:

- The individual supplies a copy of a legal, valid photo ID. The RA is to make a copy of the documentation.
- The /email= field is verified during the registration process. The requester have to prove that he has access to the mailbox and that he can use it to receive mail.

3.2.4 Non-verified subscriber information

All subscriber information required has to be duly verified. Additional information given by the subscriber can be ignored.

3.2.5 Validation of Authority

Whenever an individual's name is associated with an Organization name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the TN PKI RA:

- Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with

the applicable government that confirms the existence of the organization, and

- Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.

3.2.6 Criteria for Interoperation

The Tunisian National Root CA and its subsidiaries support multiple registration and certification authorities. In order to become an authorized registration or certification authority, the respective authority signs a contractual agreement with the National Digital Certification Agency binding them to this CP/CPS and ensuring that all the processes and procedures of the authority meet the minimum requirements specified in this CP/CPS.

The requirements to be met by the authority are included but are not limited to:

- Signing a contractual agreement with the National Digital Certification Agency,
- Being compliant with the stipulations of this CP/CPS,
- Having passed and keeping current a WebTrust or ETSI audit,
- Publishing its own CP/CPS.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The TN PKI CA certificate re-key follows the same procedure as that of the initial key generation. Subscriber certificates are not be subject for re-key. A new certificate with new keys is generated based on initial issuing process.

3.3.2 Identification and authentication for re-key after revocation

After a certificate has been revoked other than during a renewal or update action, the subscriber is required to go through the initial registration process described in Section 3.2 (Initial Identity Validation) above to obtain a new certificate with new keys.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

Below is a list of people who can submit certificate applications:

(a) Any individual who is the subject of the certificate;

(b) Any authorized representative of a juridical entity or organization;

(c) Any authorized representative of a CA; or

(d) Any authorized representative of a RA.

4.1.2 Enrollment process and responsibilities

The Tunisian National Root CA and its subsidiaries maintain systems and processes that sufficiently authenticate the Applicant's identity for all Certificate types. Applicants submit sufficient information to allow the TN PKI RA to successfully perform the required verification. The TN PKI CAs and RAs protect communications and securely store information presented by the Applicant during the application process in compliance with the National Digital Certification Agency Security Policy.
Generally, the application process includes the following steps (but not necessarily in this order as some workflow processes generate Key Pairs after the validation has been completed):

- Generating a suitable Key Pair using a suitably secure platform;
- Generating a Certificate Signing Request (CSR) using an appropriately secure tool;
- Submitting a request for a Certificate type and appropriate application information;
- Agreeing to a Subscriber Agreement or other applicable terms and conditions; and
- Paying any applicable fees.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The identification and authentication of an applicant for a certificate meet the requirements specified in Section 3.2 (Initial Identity Validation) of this CP/CPS.

The TN PKI CA or RA identify and authenticate all required subscriber information in terms of Section 3.2 (Initial Identity Validation).

4.2.2 Approval or Rejection of Certificate Applications

The TN PKI CA will approve an application for a certificate if the following criterias are met:

- Successful identification and authentication of all required Subscriber information in terms of section 3.2
- Payment has been received

The TN PKI CA will reject a certificate application if:

- Identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request, or
- The Subscriber fails to respond to notices within a specified time, or
- Payment has not been received.

4.2.3 Time to process certificate applications

After receiving the registration form as well as the complete, accurate registration documentation, the time to process certificate applications is two working days.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Upon receipt of an approved certificate signing request, the TN PKI CA will verify:

- the integrity of the request;
- the authenticity and authority of the RA operator;
- the contents of the certificate requests for compliance with the technical specification as outlined in section 7.1.2.

On successful verification, the concerned CA will then issue the requested certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The CA may notify the requester in different ways:

- If the certificate is presented to the subscriber immediately, special notification may not be necessary.
- The CA may:
  - email the certificate to the subscriber,
  - email the certificate to the requesting RA,
  - email information permitting the subscriber to download the certificate from a web site or repository,
  - email information permitting the RA to download the certificate from a web site

or repository.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The subscriber is responsible for installing the issued certificate on the subscriber's computer or security module according to the subscriber's system specifications. A subscriber is deemed to have accepted a certificate when:

- The subscriber uses the certificate; or
- 30 days pass since issuance of the certificate.

4.4.2 Publication of the certificate by the CA

As specified in Section 2 (Publication and Repository Responsibilities) of this CP/CPS, the CA may publish the Certificate into a directory such as LDAP.

4.4.3 Notification of certificate issuance by the CA to other entities

TN PKI CAs/ RAs may be informed of the issuance if they were involved in the initial enrollment.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers have to protect their Private Key taking care to avoid disclosure to third parties. Each CA under the Tunisian National Root CA provides a suitable Subscriber Agreement which highlights the obligations of the Subscriber with respect to Private Key protection.
Subscriber use private keys in accordance with the key usage field extension. End-user subscriber is bound to use the certificate for its lawful and intended purposes only.
Where it is possible to make a backup of a Private Key, Subscribers must use the same level of care and protection attributed to the live Private Key. At the end of the useful life of a Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup.

4.5.2 Relying Party Public Key and Certificate Usage

Within this CP/CPS, the TN PKI CA 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. The CA provides a Relying Party agreement to Subscribers, the content of which is presented to the Relying Party prior to reliance upon a Certificate from an issuing CA.

Software used by Relying Parties are fully compliant with X.509 standards including best practice for chaining decisions around policies and key usage.

4.6 Certificate renewal

Certificate renewal is a process in which a new certificate is issued to a subscriber. The certificate contains new validity information, but retains subject and key information.
The process of certificate renewal is not supported by the TN PKI RA. Tje RA limits the validity period of certificates to ensure that keys are used only during a stipulated period of time.

4.6.1 Circumstances for Certificate Renewal

As indicated in section 4.6 TN PKI does not support renewal..

4.6.2 Circumstance for certificate renewal

As indicated in section 4.6 TN PKI does not support renewal..

4.6.3 Who may request renewal

End-user certificates is not subject for renewal.

4.6.4 Processing certificate renewal requests

As indicated in section 4.6 TN PKI does not support renewal.

4.6.5 Notification of new certificate issuance to subscriber

As indicated in section 4.6 TN PKI does not support renewal.

4.6.6 Conduct constituting acceptance of a renewal certificate

As indicated in section 4.6 TN PKI does not support renewal.

4.6.7 Publication of the renewal certificate by the CA

As indicated in section 4.6 TN PKI does not support renewal.

4.6.8 Notification of certificate issuance by the CA to other entities

As indicated in section 4.6 TN PKI does not support renewal.

4.7 Certificate Re-Key

Re-keying a certificate means to request a new certificate with the same certificate contents except for a new Public Key. Only valid certificates can be rekeyed. All re-keys are done manually.

4.7.1 Circumstance for certificate re-key

Prior to the expiration of an existing certificate, a certificate may renew its keys if it deemed necessary regarding to one of the following reasons:

a) Migration of hardware;

b) The keys have to low cryptographic strength;

c) The keys have high exposure; or

d) Enforced by standards or applications.

End-user Subscriber certificates are not subject for re-key. A new certificate with new keys are generated based on initial issuing process.

4.7.2 Who may request certification of a new public key

Authorized representatives of TN PKI CAs may request for re-key of their CA certificates.

End-user Subscriber certificates are not subject for re-key. A new certificate with new keys are generated based on initial issuing process.

4.7.3 Processing certificate re-keying requests

The TN PKI CA will verify

- the integrity of the request;
- verify the contents of the certificate requests for compliance with the technical specification as outlined in section 7.1.2.

On successful verification, the TN PKI CA will then issue the requested certificate.

4.7.4 Notification of new certificate issuance to subscriber

TN PKI CA/RA operating under this CP/CPS may inform the Subscriber of the issuance of re-keyed certificates as specified in Section 4.3.2 (Notification to Subscriber by the CA of Issuance of Certificate) of this CP/CPS.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Conduct constituting acceptance of a re-keyed certificate is in accordance with Section 4.4.1 (Conduct Constituting Certificate Acceptance) of this CP/CPS.

4.7.6 Publication of the re-keyed certificate by the CA

As specified in Section 2 (Publication and Repository Responsibilities) of this CP/CPS, all certificates are published in the TN PKI CA's repository system.

4.7.7 Notification of certificate issuance by the CA to other entities

A TN PKI CA/RA operating under this CP/CPS may choose to notify other CAs or RAs of the certificate issuance.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

Certificate modification is the process through which a subscriber requests a certificate with modified subject information. The TN PKI RA treats these requests as initial registration requests. The subscriber is therefore required to start a new certificate request.

Certificate modification may occur regarding to one of the following reasons:

(a) Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the end-user Subscriber's public key). Certificate modification is considered a Certificate Application as stated in Section 4.1 (Certificate Application).
(b) Certificate modification is performed when change occurs in any of the information of an existing certificate. After modification, the original certificate are revoked.
(c) End-user Subscriber certificates are not subject for modification. A new certificate with new keys are generated based on initial issuing process.

4.8.2 Who may request certificate modification

Principles of Section 4.1.1 apply.

4.8.3 Processing certificate modification requests

Principles of Section 3.2 apply.

4.8.4 Notification of new certificate issuance to subscriber

Principles of Section 4.3.2 apply.

4.8.5 Conduct constituting acceptance of modified certificate

Principles of Section 4.4.1 apply.

4.8.6 Publication of the modified certificate by the CA

Principles of Section 4.4.2 apply.

4.8.7 Notification of certificate issuance by the CA to other entities

Principles of Section 4.4.3 apply.

4.9 Certificate revocation and suspension

With regard to CRL, the Tunisian National Root CA will adhere to these general guidelines:

- Certificates that have been revoked can never be "unrevoked".
- Certificates that have once been published on a CRL will always remain on the CRL.

4.9.1 Circumstances for revocation

A certificate is revoked when the bind between the subject and the subject's public key is no longer valid. There are several circumstances under which a TN PKI CA certificate will be revoked:

a) Key Compromise: The TN PKI CA private key has been compromised;

b) TN PKI CA Compromise: The NDCA CA database has been compromised;

c) The TN PKI CA is not compliant with its CP/CPS;

d) Cessation of Operation: The TN PKI CA cease operation;

An end-user subscriber certificate can be requested for revocation under any of the following conditions:

a) When a verified request for revocation is received by TN PKI CA or RA;

b) When any of the information found in the certificate is changed or no longer applicable;

c) When the Private Key, or the media holding the Private Key, associated with the certificate is compromised;

d) When the TN PKI CA determines that the end-user entity is no longer complying with the requirements of this CP/CPS; or

e) When the TN PKI CA has the reason to believe that the certificate was issued in a manner that is not in accordance with the procedures required by this CP/CPS.

4.9.2 Who can request revocation

All subsidiaries of this CA accept certificate revocation requests from the following:

- the owner of the profile used to issue the initial registration request,
- the owner of the private key,
- an authorized representative of the organization that has approved the content of the /O= field in the certificate,
- a properly authorized CAO,
- a Tunisian court of law.

Only the TN PKI is entitled to request or initiate the revocation of the certificate issued to its own CAs.

4.9.3 Procedures for revocation request

Any one of these procedures can be used to successfully revoke a certificate:

- The owner of the private key can revoke this certificate on line.
- By using a revocation form, the subscriber can issue an off line revocation request in writing. Such a request, in order to be authorized, carry the personal signature of the original requester of the certificate as well as proof of identity.
- The subscriber can personally visit the RA offices and request the revocation of a certificate off line. The subscriber presents a piece of identification. For identification purposes TN PKI RA will accept any government issued photo identification document.

All registrations authorities operating under this CP/CPS adhere to the following stipulations:

Online revocation management services are available 24 hours per day, 7 days per week.

Offline revocation management services are available and be able to receive revocation requests during business hours. Revocation requests transmitted on paper are taken into evaluation immediately during working hours and necessary actions are carried out within at most 24 (twenty four) hours.

4.9.4 Revocation request grace period

No grace period is permitted once a revocation request has been verified. RAs will revoke certificates as soon as reasonably practical following verification of a revocation request.

4.9.5 Time within which CA must process the revocation request

All certificate revocation requests are executed without delay.

4.9.6 Revocation checking requirement for relying parties

Relying parties validate any presented certificate against the most updated CRL as minimum. Alternatively, relying parties may check certificate status using OCSP. TN PKI CA provide relying parties with information on how to find the appropriate CRL or OCSP responder to check for revocation status.

4.9.7 CRL issuance frequency

The CRLs of the Tunisian National Root are issued at least once a year or upon sub-root certificate revocation.

The CRLs of the intermediate CAs are issued at least once a year or upon issuing CA certificate revocation.

The CRL of the issuing CAs are issued every twenty four (24) hours or whenever a certificate is revoked.

The OCSP responder will report a certificate revoked immediately after the revocation has been completed.

4.9.8 Maximum latency for CRLs

The CRL of this CA and all its subordonates are issued according to section 4.9.7 and published in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.

4.9.9 On-line revocation/status checking availability

The Tunisian National Root CA and all its subsidiaries support the OCSP protocol for on line revocation checking. The OCSP responder URL is stored in every certificate issued by one of the subsidiaries of the Tunisian National Root CA (field “Authority Info Access”).

TN PKI provides uninterrupted on-line certificate status protocol OCSP support. By this OCSP service which is a real time certificate status inquiry and more reliable than CRLs, the status of certificates may be inquire on-line by appropriate software on the customer side. It is possible by this inquiry to obtain information about the status of a certificate at any specific time (valid, revoked, unknown).

Within the scope of TN PKI OCSP service, the responses sent to the client systems are signed using the OCSP responder certificates that are generated for the purpose of signing OCSP responses. Any response for a certificate issued by TN PKI is signed using an OCSP responder certificate that is issued by the root certificate or the intermediates CAs certificates or the issuing CAs certificates that issued the queried certificate.

4.9.10 Online revocation checking requirements

Relying parties must, when working with certificates issued by TN PKI CAs, at all times verify them. It is recommended that relying people when inquiring the status of certificates prefer OCSP if their technical capabilities allow, or opt for CRL as a second alternative.

4.9.11 Other forms of revocation advertisements available

TN PKI does not employ any method other than OCSP and CRL for advertising revocation status.

4.9.12 Special requirements regarding key compromise

If a subscriber knows or suspects that the integrity of his certificate's private key has been compromised, the subscriber:

- immediately cease using the certificate,
- immediately initiate revocation of the certificate,
- delete the certificate from all devices and systems,
- inform all relying parties that may depend on this certificate.

The compromise of the private key may have implications on the information protected with this key. The subscriber must decide how to deal with the affected information before deleting the compromised key.

4.9.13 Circumstances for suspension

Suspension is not applicable for end-user certificate. After completing the secondary identity verification, revocation process is completed.
For root or sub-root certificates of TN PKI suspension is not performed.

4.9.14 Who can request suspension

Certificates may not be suspended.

4.9.15 Procedure for suspension request

Certificates may not be suspended.

4.9.16 Limits on suspension period

Certificates may not be suspended.

4.10 Certificate status services

4.10.1 Operational characteristics

TN PKI issuing CAs publish CRLs once a day within 24 (twenty four) hour intervals with a validity period of 24 (twenty four) hours even if there is no change in the status of certificates. Only exception to the validity period of CRL is the expiry date of root or subsidiaries CA certificates. Expiry date of a root or a subsidiary certificate is written to the NextUpdate field of the CRL if the next update of the CRL exceeds the validity period of a root or a subsidiary certificate.

TN PKI provides on-line certificate status protocol OCSP support. It is possible by this inquiry to obtain real time information on the status of a certificate any time (good, revoked or unknown).

4.10.2 Service availability

Certificate status services are available 24 hours per day, 7 days per week.

TN PKI RA provides customers with pre-filled revocation request forms during the registration process. TN PKI RA guarantees timely processing of revocation requests without undue delay if these forms are sent through registered mail and if all required signatures are present.

4.10.3 Optional features

The TN PKI certificate status services do not include or require any additional features.

4.11 End of subscription

An end-user subscriber may end a subscription for his certificate by:
a) Allowing its certificate to expire without renewing or re-keying that certificate;
b) Revoking of its certificate before certificate expiration.

4.12 Key escrow and recovery

The private keys for each CA certificate were generated and are stored in Hardware Security Modules (HSM) and are backed up but not escrowed.

4.12.1 Key escrow and recovery policy and practices

The TN PKI CA key-recovery is based on HSM standard key-backup where the keys in the backup are protected with encryption. All HSM backups and administrator smartcards are stored in a safety vault. Only persons performing trusted roles have the access to the safety vault.

The TN PKI does not store copies of subscriber private keys; a key escrow is not possible.

4.12.2 Session key encapsulation and recovery policy and practices

The Tunisian National Root CA and its subordinates do not support session key encapsulation.

5 Facility, management, and operational controls

This section of the CP/CPS outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use by the TN PKI to provide trustworthy and reliable CA operations.
The National Digital Certification Agency has implemented a Security Policy, which supports the security requirements of this CP/CPS. Compliance with these policies is included in independent audit requirements described in section 8.

5.1 Physical controls

5.1.1 Site location and construction

CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information.
The construction of the NDCA's site complies with the regulations and standards, and incorporates the results of a risk analysis and specific requirements to face accidental risks.

5.1.2 Physical access

Three layers of physical security exist between the outside of the building and the TN PKI CAs operations. Access to the secure part of TN PKI facilities is limited through the use of physical access control and is only accessible to appropriately authorized individuals. TN PKI employees use access badges imprinted with a serial number to record ingress and egress through controlled access doors located throughout the facility.
During regular business hours, entry to the building where the CAs are housed is accessed through a reception area with a receptionist on duty. A security guard is also on duty at the facility 24 hours a day, 7 days a week, and 365 days a year.
Access to all areas beyond the reception area requires the use of an access card. All access card use is logged. The building is equipped with motion detecting sensors, and the exterior and internal passageways of the building are also under constant video surveillance.

Access to the Data Center housing the CAs platforms requires dual control. In fact, the doors to the room are equipped with biometric access control authenticators.

5.1.3 Power and air conditioning

The Data Center has primary and secondary power supplies that ensure continuous, uninterrupted access to electric power. Redundant backup power is provided by battery uninterrupted power supplies (UPS) and one generator.

The Data Center is equipped with heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

TN PKI has taken reasonable precautions to minimize the impact of water exposure to its Data Center.

5.1.5 Fire Prevention and Protection

TN PKI has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. TN PKI's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information are stored within TN PKI facilities with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage such as water, fire, and electromagnetic.

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturer s' guidance prior to disposal.

5.1.8 Off-Site Backup

TN PKI performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a bonded third party storage facility and TN PKI's disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

TN PKI personnel in trusted roles include, but are not limited to, CA and system administration personnel and personnel involved with customer support and vetting. An additional role external to TN PKI is the Auditor role, performed by TN PKI 's auditor in accordance with section 8 below.

The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the TN PKI.

Registration and Customer Services Responsible
Employees responsible for routine certification services such as customer services, document control, processes relating to certificate registration, generation and revocation. These employees are trusted roles.

PKI Administrator
The PKI Administrator is a trusted role. He is responsible for the installation and configuration of the different components of the PKI (CA, RA, TMS, ...).

System Administrator
The TN PKI System Administrator is a trusted role. He is responsible for the installation and configuration of the system hardware, including servers, routers, firewalls, and network configurations. The System Administrator is also responsible for keeping systems updated with software patches and other maintenance needed for system stability and recoverability.

Physical Security Officer
The Physical Security Officer is a trusted role. He is responsable for the installation and configuration of the physical security platforms (access control, video surveillance, IDS, ...)

Logical Security Officer
The Security Officer is a trusted role. He is responsable for the installation and configuration of the physical logical security plateforms (firewalls, WAF, ...).

Customer Support Personnel
Customer support and vetting personnel serve in a trusted role. They are responsible for interacting with Applicants and Subscribers, managing the certificate request queue and completing the certificate approval checklist as identity vetting items are successfully completed.

System Auditor
The System Auditor is a trusted role. He is authorized to view archives and audit logs of the trustworthy system.

5.2.2 Number of persons required per task

Two or more persons are required for TN PKI CAs for the following tasks:

(a) CA key generation = Three (3) persons
(b) CA signing key activation = Three (3) persons
(c) CA private key backup = Three (3) persons

Where multiparty control for logical access is required, at least one of the participants is an administrator. All participants must serve in a trusted role as defined in Section 5.2.1 (Trusted Roles).

Multiparty control for logical access are not achieved using personnel that serve in the Auditor Trusted Role.
HSM Administrators uses HSM Smartcards for authentication. The HSM itself enforces dual control based on the HSM smartcards for the different functions. The number of needed HSM-smartcards (m) of the total number of produced HSM-smartcards (n) will be:

(a) Key generation = 3 of 6
(b) Signing key activation = 3 of 8
(c) Private key backup and restore = 3 of 6

End-user certificate issuance requires the approval of at least two persons.
End-user Certificate revocation requires the approval of at least two persons.

5.2.3 Identification and authentication for each role

TN PKI personnel in trusted roles first authenticate themselves before they are allowed access to the components of the system necessary to perform their trusted roles.
For normal operations systems, access is controlled by user account and password, IP address subnet, and SSL. These mechanisms restrict access to those who are authorized and make actions directly attributable to the individual taking such action while fulfilling the trusted role.

5.2.4 Roles requiring separation of duties

While the certification process is operated, the entirety of sequential operations made on the same certificate are performed by different persons at different process points. Duties have been distributed to separate roles and thereby a single person is prevented from performing the entirety or a large part of the work in the process. Each operation is logged so as to include detailed place and time data based on roles. Specifically, a user that is authorized to assume a Security Officer or Registration and Customer Services Officer role is not authorized to assume a System Auditor role. A user that is authorized to assume a System Administrator role is not authorized to assume a Security Officer or a System Auditor role.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The National Digital Certification Agency requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances.

The technical Team of TN PKI demonstrate understanding of security in general and expert knowledge of IT security in particular.

Before starting work at TN PKI, new staff members have to sign confidentiality (non-disclosure) agreements and independence statements.

5.3.2 Background check procedures

The National Digital Certification Agency verifies the background of its employees covering the following areas:

(a) Employment

(b) Education and Certification

(c) Place of residence

(d) Law Enforcement

(e) References

The National Digital Certification Agency will not appoint any person who is known to have been convicted of a serious crime or other offense which could affect his suitability for the position. Personnel don't have access to the trusted functions until all necessary checks have been completed. TN PKI will ask any candidate to provide such information and refuse an application if access to such information is denied.

5.3.3 Training requirements

TN PKI provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily.

TN PKI maintains records of such training. TN PKI periodically reviews and enhances its training programs as necessary.
TN PKI's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- Security and operational policies and procedures,
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining frequency and requirements

Retraining of employees is done as necessity arises, depending on the needs of the organization or the needs of the individual.

Individuals responsible for PKI roles are aware of changes in the TN PKI CAs operation. Any significant change to the operations have a training (awareness) plan, and the execution of such plan are documented. Examples of such changes are software or hardware upgrade, changes in automated security systems and relocation of equipment.

5.3.5 Job rotation frequency and sequence

Job rotation of employees is done as necessity arises, depending on the needs of the organization, or by request of an individual employee.

5.3.6 Sanctions for unauthorized actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of TN PKI policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to the TN PKI employees in a comparable position.

Independent contractors and consultants who have not completed or passed the background check procedures specified in section 5.3.2 are permitted access to NDCA's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

In addition, TN PKI require a confidentiality agreement covering the contractual relations with third-party contractors.

5.3.8 Documentation Supplied to Personnel

TN PKI personnel involved in the operation of TN PKI's services are required to read this CP/CPS and the Security Policy. TN PKI provides its employees the requisite documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The TN PKI manually or automatically logs the following events:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
    a. Certificate requests, renewal, and re-key requests, and revocation;

b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
d. Acceptance and rejection of certificate requests;
e. Issuance of Certificates; and
f. Generation of Certificate Revocation Lists and OCSP entries.

3. Security events, including:
   a. Successful and unsuccessful PKI system access attempts;
   b. PKI and security system actions performed;
   c. Security profile changes;
   d. System crashes, hardware failures, and other anomalies;
   e. Firewall and router activities; and
   f. Entries to and exits from the CA facility.

More details are introduced in the event logging procedure of TN PKI.

5.4.2 Frequency of processing log

The CA system is continuously monitored to provide real time alerts of significant security and operational events for review by designated system administrator. The event log processing frequency is described in event logging procedure of TN PKI.

5.4.3 Retention Period for Audit Log

The CA saves electronic certification service audit logs properly. The preservation period of audit log is described in event logging procedure of TN PKI.

5.4.4 Protection of Audit Log

The TN PKI CA's system configuration and procedures are implemented together to ensure that:

(a) Only personnel assigned to trusted roles have read access to the logs;
(b) Only authorized people may archive audit logs; and,
(c) Audit logs are not modified.

The person performing audit log archive need not have modify access, but procedures are implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).

5.4.5 Audit Log Backup Procedures

The backups of audit logs are created daily and full backups as is described in the backup procedure of TN PKI.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by TN PKI personnel.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

The TN PKI CA assess the vulnerability of its CA system or its components annually. A routine assessment of the PN PKI CA system is performed regularly for evidence of any malicious activity.

5.5 Records archival

5.5.1 Types of records archived

The following records are archived:

- a daily backup of any information that this CA and its subsidiaries produce
- registration information of end entities

5.5.2 Retention period for archive

Archived information is kept at least 20 years beyond the end of subscription, as specified in the archiving procedure.

5.5.3 Protection of archive

Protection of the archive is as follows:

- Archived information is only accessible to authorized TN PKI employees according to the role model as presented in section 5.2.
- Protection against deletion: The RA archive (physical documents) is stored in a safe deposit and can only be accessed by authorized TN PKI employees as detailed in the role model presented in 5.2.
- Protection against the deterioration of the media on which the archive is stored: Digital data is to be migrated periodically to fresh media.

- Protection against obsolescence of hardware, operating systems, and other software: As part of the archive, the hardware (if necessary), operating systems, and/or other software is archived in order to permit access to and use of archived records over time.

More details are in the archiving procedure of TN PKI.

5.5.4 Archive backup procedures

Archived information is stored off-site in safe deposit at the secondary site of TN PKI.

5.5.5 Requirements for time-stamping of records

All records in the database and in log files are time-stamped using the system time of the system where the event is recorded.

The system time of all servers is synchronized with the time source of the NTP server of TN PKI.

5.5.6 Archive collection system (internal or external)

Archive collection systems are internal. The TN PKI archive data are copied to additional media for processing. Reviewing will be done by the TN PKI CA itself.

5.5.7 Procedures to obtain and verify archived information

In the event of a court order, a high-quality copy is made of the archived information and the original is temporarily made available to the court. When the original information is returned, the high-quality copy is destroyed. This process is logged and audited.

5.6 Key changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, the National Digital Certification Agency ceases using its expiring CA Private Key to sign Certificates (well in advance of expiration) and uses the old Private Key only to sign CRLs. A new CA signing key pair is commissioned and all subsequently issued certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The TN PKI establishes business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or Compromise the CA services.
The TN PKI carries out risk assessments to evaluate business risk and determine the necessary security requirements and operational procedures to be taken as a consequence of its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary (threat evolution, vulnerability evolution, etc). This business continuity is included in the scope of the audit process as described in section 8 to validate which operations are first restored after a disaster and the recovery plan.
The TN PKI personnel that serve in a trusted role and operational role are specially trained to operate according to procedures defined in the disaster recovery plan for business critical operations.
If the CA detects a potential hacking attempt or another form of compromise, it performs an investigation in order to determine the nature and the degree of damage. Otherwise, the CA assesses the scope of potential damage in order to determine whether the CA or RA system needs to be rebuilt, whether only some Certificates need to be revoked, and/or whether a CA hierarchy needs to be declared as Compromised. The CA disaster recovery plan highlights which services are maintained (for example, revocation and Certificate status information).

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

If any equipment is damaged or rendered inoperative but the Private Keys are not destroyed, the operation is reestablished as quickly as possible, giving priority to the ability to generate Certificate status information according to the TN PKI's disaster recovery plan.

5.7.3 Entity Private Key Compromise Procedures

In the event that a TN PKI CA private key has been or is suspected to have been compromised, TN PKI personnel will immediately convene an emergency Incident Response Team to assess the situation and to determine the degree and scope of the incident and take appropriate action. The following actions outline as follows:

a) Collect all information related to the incident (and if the event is ongoing, ensure that all data are being captured and recorded);
b) Begin investigating the incident and determine the degree and scope;
c) The Incident Response Team determines the course of action or strategy that should be taken (and in the case of Private Key compromise, determining the scope of certificates that must be revoked);

d) Contact law enforcement, and other interested parties and activate any other appropriate additional security measures;
e) Monitor system, continue the investigation, ensure that all data is still being recorded as evidence and make a forensic copy of data collected;
f) Isolate, contain and stabilize the system, applying any possible short-term fixes needed to return the system to a normal operating state;
g) Prepare an incident report that analyzes the cause of the incident and implement a long term solutions.

A new CA Key Pair should be generated and a new CA Certificate should be signed in accordance with the procedures outline in Section 6 (Technical Security Controls) of this CP/CPS.

a) If the TN PKI CA distributes its Key in a self-signed certificate, the new self-signed certificate is distributed as specified in Section 6.1.4 (CA Public Key Delivery to Relying Parties) of this CP/CPS.
b) The TN PKI CA governing body is also investigate and report what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business Continuity Capabilities After a Disaster

The TN PKI CA operates a backup site, whose purpose is to ensure continuity of operations in the event of failure of the primary facility or site and mitigate the effects of any kind of natural or man-made disaster. The Disaster Recovery Plan is regularly tested, verified and updated to be operational in the event of a disaster. The TN PKI CA operations is designed to restore full service within six (6) hours of main site system failure.

5.8 CA or RA Termination

In case of termination of CA operations for any reason whatsoever, the National Digital Certification Agency will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, TN PKI will where possible take the following steps:

Provide subscribers of valid certificates with ninety (90) days notice of its intention to cease acting as a CA.

- Revoke all certificates that are still un-revoked or un-expired at the end of the ninety (90)-day,
- Notice period without seeking Subscriber's consent.
- Give timely notice of revocation to each affected Subscriber.
- Make reasonable arrangements to preserve its records according to this CP/CPS.

- Reserve its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as TN PKI's.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

6 Technical Security Controls

6.1 Key pair generation and installation

The TN PKI CA private keys are protected within a hardware security module (HSM) meeting at least Level 3 of the Federal Information Processing Standard 140-2 (FIPS 140-2). Access to the HSM within the CA environment is restricted by the use of smartcard. The HSM is always stored in a physically secure environment and subject to security controls throughout its lifecycle.

6.1.1 Key pair generation

The TN PKI CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using trustworthy systems and processes that provide for the security and required cryptographic strength for the generated keys.

The key pair for the Tunisian National Root CA has been created in a Hardware Security Module that have EAL 4+ and FIPS 140-2 Level 3.

The key pairs for the intermediate CAs have been generated in a Hardware Security Module that have EAL 4+ and FIPS 140-2 Level 3.

The key pairs for the issuing CAs have been generated in a Hardware Security Module that have EAL 4+ and FIPS 140-2 Level 3.

TN PKI HSMs are kept and operated under physical and electronic protection against all types of intervention. The secure backup of the data in HSMs are taken and stored according to the procedures. Thus when an HSM completes its physical and economic lifetime, the private keys on the HSM are destroyed as described in Section 6.2.10 while keeping the relevant backups in other media to be used in new HSM devices.

All the TN PKI CA keys are generated in pre-planned Key Generation Ceremonies. The activities performed in each key generation ceremony are recorded, dated and signed by individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate.

For certificate of devices, the generation of the end-user subscriber key pairs is generally performed by the subscriber.

For certificate of persons, the generation of the end-user subscriber key pairs is generally performed by the RA under a secure device which meets at least FIPS 140-2 level 3.

6.1.2 Private key delivery to subscriber

If a subscriber generates its own key pairs, then there is no need to deliver private keys and this section does not apply.

If a TN PKI CA or RA generates the keys on behalf of the subscriber, then the private key is delivered to the subscriber. Private keys may be delivered on a hardware security token or a smartcard. In all cases, the following requirements are met:

a) Anyone who generates a private signing key for a subscriber does not retain any copy of the key after delivery of the private key to the subscriber.

b) The private key is protected from activation, compromise or modification during the delivery process.

c) The subscriber acknowledges receipt of the private key. The TN PKI RA maintains a record of the subscriber acknowledgement of receipt of the private key.

6.1.3 Public key delivery to certificate issuer

In case of device certificate, upon making a certificate application, the Subscriber is solely responsible for generating an RSA key pair and submitting it to TN PKI in the form of a PKCS#10 CSR. Typically, SSL Certificate requests are generated using the key generation facilities available in the Subscriber's webserver software.

In case of person certificate, RAs submit the public key to the concerned CA for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) in a session secured by Secure Sockets Layer / Transport Layer Security (SSL/TLS).

Delivery of the public key occurs during the enrollment session where the applicant provides all certificate application details.

6.1.4 CA public key delivery to relying parties

All Tunisian National PKI CAs in the hierarchy makes their Certificates available to Subscribers and Relying Parties through a repository. The Tunisian National PKI generally provides the full certificate chain (including the Issuing CA and any CAs in the chain) to the end-user or relying parties.

Relying Parties may also obtain TNPKI CA Certificates containing its Public Key from the TNPKI repository.

6.1.5 Key sizes

TN PKI generates and uses a 2048-bit RSA Key with Secure Hash Algorithm version 2 (SHA-256) to sign the end-user certificates and the CRLs that it issues. TN PKI recommends that

subscribers submit 2048-bit keys to RA, and may at its discretion reject certificate requests generated with a key pair size of 1024 bits or less.

For the CA certificates, TN PKI will use the following key sizes:

- Root CA uses a 4096 bit RSA key
- All intermediate CAs uses a 4096 bit RSA key.
- All issuing CAs use 3072 bit RSA key.

6.1.6 Public key parameters generation and quality checking

Parameters can be selected by requesters, but are verified by the RA and the CA. For keys generated, all TN PKI CAs use standard parameters.

No stipulations can be made for browser-generated key pairs or for key pairs imported from external sources.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The signing keys of TN PKI CAs are the only keys permitted for signing certificates and CRLs and have the keyCertSign and CRLSign key usage bit set.

Subscribers can obtain certificates that may have one or more of the following key usage bits included:

- digitalSignature
- nonRepudiation
- keyAgreement
- keyEncipherment
- DataEncipherment

Subscribers can obtain certificates issued by the issuing CAs with the following extended key usages included:

- Server Authentication
- Client Authentication
- Code Signing
- Email Protection
- Time Stamping
- OCSP Signing
- Microsoft Individual Code Signing (msICS)
- Microsoft Commercial Code Signing (msCCS)
- Microsoft Trust List Signing (msTLS)
- Microsoft Encrypted Files System (msEFS)

- Microsot Smart Card Logon (msSCL)
- IPSec End System
- IPSec Tunnel
- IPSec User

6.2 Private Key Protection and Cryptographic Module Engineering Controls

All the TN PKI CAs has implemented a combination of physical, logical, and procedural controls to ensure the security protection and prevent the loss, damage, disclosure, modification or unauthorized use of their private keys.

6.2.1 Cryptographic module standards and controls

The following list shows how the requirements for the different users of hardware cryptographic modules are implemented:

- Root CA keys : The HSM used for CA keys meets FIPS 140-1 level 3 and EAL4+ requirements.
- Intermediate CAs keys: The HSM used for CA keys meets FIPS 140-1 level 3 and EAL4+ requirements.
- Issuing CAs keys: The HSM used for CA keys meets FIPS 140-1 level 3 and EAL4+ requirements.
- Subscriber keys:
    - Certificate of devices: The subscriber is fully responsible for its private keys
    - Certificate of persons: The TN PKI uses a hardware cryptographic module where the subscriber keys are generated and stored. This hardware for key pair generation and private key storage of end-user Subscribers is, at a minimum, rated at FIPS 140-2 Level 2.

6.2.2 Private key (n out of m) multi-person control

All the TN PKI CAs has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive TN PKI CA cryptographic operations.

A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a TN PKI CA private key stored on the module.

The following list shows how multi-person controls are implemented:

- Root CA keys : Root CA keys can only be accessed on the physical and on the logical level by adhering to '3 out of 6' control, meaning that 3 of the 6 persons are present.

- Intermediate CA keys: Intermedistae CA keys can only be accessed on the physical and on the logical level by adhering to '3 out of 6' control, meaning that 3 of the 6 persons are present.
- Issuing CAs keys Management access to these keys is only possible using '4-eye' principle (2 out of m). Once the issuing CA is operable, signing operations can be authorized by a single RA operator.
- Subscriber keys: The subscriber has single-person control of the subscriber keys.

6.2.3 Private key escrow

The following list shows how private key escrow is implemented:

- Root CA keys: Root CA keys are not in escrow.
- Intermediate CA keys: The intermediate CAs keys are not in escrow.
- Issuing CA keys: The issuing CA keys are not in escrow.

6.2.4 Private key backup

The following list shows how private key backup is implemented:

- Root CA keys : Root CA key have been backed up into a HSM so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 6 persons be present in order to gain physical and logical access.
- Intermediate CA keys: Intermediate CAs keys have been backed up into a HSM so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 6 persons be present in order to gain physical and logical access.
- Issuing CA keys: The Issuing CAs keys have been put into a HSM, so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 6 persons be present in order to gain physical and logical access.
- Subscriber keys: All the TN PKI CAs do not store copies of subscriber private keys. Subscribers are solely responsible for backup of their private keys. For the backup of subscriber private keys, subscribers may choose to backup their keys to their hard drive. The TN PKI CAs store only subscribers private keys related to enciphrment certificates.

6.2.5 Private key archival

The following list shows how private key archival is implemented:

- Root CA keys: The Root CA keys are not archived.
- Intermediate CAs keys: The intermediate CAs keys are not archived.
- Issuing CA keys: The Issuing CA keys are not archived.

- Subscriber keys: Only subscribers private keys related to enciphrment certificates are archived.

6.2.6 Private key transfer into or from a cryptographic module

The following list shows how private key transfers are implemented:

- Root CA keys : The Root CA keys can be cloned from the master HSM to other HSM. This is achieved in a cloning ceremony.
- Intermediate CAs keys: The intermediate CAs keys are cloned in the same manner as Root keys.
- Issuing CAs keys: The Issuing CAs keys are cloned in the same manner as Root keys.
- Subscriber keys: Subscribers or the TN PKI RA are solely responsible for the transfer of subscriber keys into or from a cryptographic module.

6.2.7 Private key storage on cryptographic module

The following list shows how private keys are stored on cryptographic modules:

- Root CA keys: The Root CA keys are stored on cryptographic modules so that they can be used only if properly activated.
- Intermediate CAs keys: The Intermediate CAs keys are stored on cryptographic modules so that they can be used only if properly activated.
- Issuing CAs keys: The issuing CAs keys are stored on cryptographic modules so that they can be used only if properly activated.
- Subscriber keys:
    - Certificate of devices: The subscriber is fully responsible for its private keys
    - Certificate for persons: The TN PKI uses a hardware cryptographic module where the subscriber keys are generated and stored.

6.2.8 Method of activating private key

All the TN PKI CAs protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure or unauthorized use.
All the TN PKI CA private keys are activated according to the specifications of the cryptographic hardware manufacturer and witnessed during the key generation or certificate signing ceremony.

The following list shows how private keys are activated:

- Root CA keys: The Root CA keys are activated with two user key (physical) and two user PIN (knowledge).

- Intermediate CAs keys: The intermediate CAs keys are activated with two user key (physical) and two user PIN (knowledge).
- Issuing CA keys: The Issuing CA keys are activated with two user key (physical) and two user PIN (knowledge).
- Subscriber keys: The subscriber private key is activated with a hardware cryptographic module PIN or only a user PIN (knowledge).

6.2.9 Method of deactivating private key

The following list shows how private keys are deactivated:

- Root CA keys: The Root CA keys are deactivated either by logging out of the HSM, by terminating the session with the HSM, by removing the CA token from the computer or by powering down the system.
- Intermediate CA keys: The intermediate CAs keys are deactivated either by logging out of the HSM, by terminating the session with the HSM, by removing the CA token from the computer or by powering down the system.
- Issuing CA keys: The Issuing CAs keys are deactivated by terminating the key daemon process, by shutting down the CA server processes or by shutting down the server.
- Subscriber keys: The subscriber is solely responsible for the deactivation of its private key.

6.2.10 Method of destroying private key

The following list shows how private keys are destroyed:

- Root CA keys: The Root CA keys are destroyed by initializing the Hardware Security Module. In cases when this initialization procedure fails, the TN PKI will physically destroy the device to remove the ability to extract any private key.
- Intermediate CAs keys: The intermediate CAs keys are destroyed by initializing the Hardware Security Module. In cases when this initialization procedure fails, the TN PKI will physically destroy the device to remove the ability to extract any private key.
- Issuing CAs keys: The issuing CAs keys are destroyed by initializing the Hardware Security Module. In cases when this initialization procedure fails, the TN PKI will physically destroy the device to remove the ability to extract any private key.
- Subscriber keys: The subscriber keys are destroyed by initializing the hardware cryptographic module.

6.2.11 Cryptographic Module Rating

Private keys of root, intermediates and issuing CAs certificates of TN PKI are generated in cryptographic hardware modules.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All certificates, and therefore the public keys of all subscribers and all CAs, are stored on line in a database. This database is replicated to all servers in the CA cluster. This database is also part of the daily backup.

6.3.2 Certificate operational periods and key pair usage periods

The usage periods for certificates issued by this CA are as follows:

- The Tunisian National Root CA is valid approximately 20 years.
- The intermediate CAs are valid approximately 15 years.
- The issuing CAs certificates are issued for a maximum life time of 10 years.
- The end-user certificates can have a lifetime of 1 or 2 or 3 years.

6.4 Activation data

6.4.1 Activation data generation and installation

The TN PKI activates the cryptographic module containing its TN PKI CAs' private keys according to the specifications of the hardware manufacturer and the Key Ceremony Document.

This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3 and EAL4+. It can only be activated through the use of HSM smart cards (3 of 6) accomplished by strong passwords.

All smart cards are stored in a safe when not in use. The cryptographic hardware is held under three-person control as explained in Section 5.2.2 (Number of Persons Required Per Task) and elsewhere in this CP/CPS.

All TN PKI personnel are required to use strong passwords and to protect PINs and passwords. The TN PKI requires that passwords to workstations be changed on a regular basis.

6.4.2 Activation data protection

- Root CA keys: The activation data is distributed over multiple physical keys. The owners of a part are required to store this part in a private safe deposit of the National Digital Certification Agency.
- Intermediate CAs keys: The activation data is distributed over multiple physical keys. The owners of a part are required to store this part in a private safe deposit of the National Digital Certification Agency.
- Issuing CAs keys: The activation data is known to trusted individuals at TN PKI. An escrow copy is stored in a safe deposit with dual controls access.
- Subscribers keys: The TN PKI recommends that subscribers store their private keys in encrypted form and protect their private keys through the use of a hardware cryptographic module (smartcard or token) and/or strong passphrase. The subscribers are obliged to keep the activation data secret at all times.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

The CA servers are protected by external firewalls that filter out all unwanted traffic. Additionally, the CA systems are hardened and equipped with a high-security operating system. SA access to the system is granted only over secure and restricted protocols using strong publickey authentication.

6.5.1 Specific computer security technical requirements

The TN PKI uses a layered security approach to ensure the security and integrity of the computers used to run the CA software. The following controls ensure the security of TN PKI operated computer systems:

- Hardened operating system.
- Software packages are only installed from a trusted software repository.
- The TN PKI CAs production network is logically separated from other components. This separation prevents network access except through defined application processes. The TN PKI uses firewalls to protect the production network from external intrusion and limit the nature and source of network activities that may access production systems.
- Authentication and authorization for all functions.

- Strong authentication and role-based access control for all vital functions.
- Monitoring and auditing of all activities.

6.5.2 Computer security rating

The National Digital Certification Agency has established a security framework which covers and governs the technical aspects of its computer security.

The systems themselves and the services running on these systems are subject to thorough reviews and testing (including penetration testing).

In order to make its environment more secure and to keep it on a state-of-the-art security level, TN PKI operates a vulnerability management process which includes monitoring of supplier security alerts.

6.6 Life cycle technical controls

6.6.1 System development controls

TN PKI has mechanisms in place to control and monitor the acquisition and development of its CA systems.

Change control processes consist of change control data entries that are processed, logged and tracked for any non-security-related changes to CA systems, equipment and software. Change requests require the approval of a committee.

In this manner, TN PKI can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management.

All hardware and software are shipped under standard conditions with controls in place to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering. Some of the PKI software components used by TN PKI to provide CA services are developed in-house or by consultants using standard software development methodologies, other software is purchased commercial off-the-shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors. Updates of equipment or software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel.

6.6.2 Security management controls

TN PKI has mechanisms in place to control and monitor the security-related configurations of its CA systems. Change control processes consist of change control data entries that are processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls. In this manner, TN PKI can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management.

6.7 Life cycle security controls

6.7.1 System Development Controls

System development controls are applied for development facility security (through facility security clearance certifications), development environment security, development personnel security, configuration management security during product maintenance and software development methodology (through ISO 9001 certifications).

Details about these aspects are documented in change management procedure and maintenance procedure.

6.7.2 Security Management Controls

Appropriate tools are used and security procedures are implemented to ensure security of the operational systems and the computer network used in TN PKI.

6.7.3 Life Cycle Security Controls

Not applicable

6.8 Network security controls

TN PKI's CA system is connected to one internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses. TN PKI's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses.

Root and intermediate CAs Keys are kept offline and brought online only when necessary to sign certificate-issuing subordinate CAs or periodic CRLs.

Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. It is TN PKI's security policy to block all ports and protocols and open only necessary ports to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. All firewall configurations and changes thereto are documented, authorized, tested and implemented in accordance with change management procedures.

TN PKI's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

6.9 Time-Stamping

TN PKI operates an internal time service using various a GPS-NTP receiver.

Based on this internal time service, TN PKI a time-stamping service that can be used to create a time-stamp for arbitrary documents.

TN PKI may charge a fee for this service. The keys used for the creation of time-stamping signatures are treated in exactly the same fashion as the keys of the subsidiaries of the Tunisian National Root CA.Certificate, CRL and OCSP Profiles

This section contains the rules and guidelines followed by the TN PKI CAs in populating X.509 certificates and CRL extensions.

7 Certificate profile

Certificate issued under this CP/CPS conform to the RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

The structure of such a certificate is:

Certificate Field	Value	Comment
Version	X.509 Version 3	See section 7.1.1
Serial number	Unique number	Will be used in CRL
Signature algorithm identifier	OID	See section 7.1.3
Validity period	Start date, expiration date	
Subject	According to X.500	See Definitions in section 1.6
Subject Public Key Info	Public Key algorithm, Subject Public Key	See section 7.1.3
Extensions	X509V3 Extensions	See section 7.1.2
Signature	Certificate Signature	

7.1.1 Version number(s)

All TN PKI CAs Certificates are X.509 version 3 certificates.

End-user Certificates is be X.509 v3.

7.1.2 Certificate Extensions

The TN PKI populates X.509 version 3 Certificates with the extensions that comply with RFC 5280.

7.1.2.1 Extensions of TN PKI CAs

Extension Attribute	Values
Tunisian National Root CA	
Serial Number	Defined by the CA

Issuer DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia National Root CA
Subject DN	C=TN, L=Tunis, O =National Digital Certification Agency, CN=Tunisia National Root CA
Not Before	YYMMDDHHMMSS (Key Ceremony date)
Not After	YYMMDDHHMMSS (Key Ceremony date) + 20y 6m
Validity	20y 6m
Key Specification	RSA 4096
Signature Algorithm	SHA256WithRSA
Tunisia Gov CA	
CA Name	Tunisia Gov CA
Issuer DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia National Root CA
Subject DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia Gov CA
Not Before	YYMMDDHHMMSS (Key Ceremony date)
Not After	YYMMDDHHMMSS (Key Ceremony date) + 15y 3m
Validity	15y 3m
Key Specification	RSA 4096
Signature Algorithm	SHA256WithRSA
Tunisia Corporate CA	
CA Name	Tunisia Corporate CA
Issuer DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia National Root CA
Subject DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia Corporate CA
Not Before	YYMMDDHHMMSS (Key Ceremony date)
Not After	YYMMDDHHMMSS (Key Ceremony date) + 15y 3m
Validity	15y 3m
Key Specification	RSA 4096

Signature Algorithm	SHA256WithRSA
TnTrust Gov CA	
Issuer DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia Gov CA
Subject DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Gov CA
Not Before	YYMMDDHHMMSS (Key Ceremony date)
Not After	YYMMDDHHMMSS (Key Ceremony date) + 10y 1m
Validity	10y 1m
Key Specification	RSA 3072
Signature Algorithm	SHA256WithRSA
TnTrust Qualified Gov CA	
Issuer DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia Gov CA
Subject DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Qualified Gov CA
Not Before	YYMMDDHHMMSS (Key Ceremony date)
Not After	YYMMDDHHMMSS (Key Ceremony date) + 10y 1m
Validity	10y 1m
Key Specification	RSA 3072
Signature Algorithm	SHA256WithRSA
TnTrust Corporate CA	
Issuer DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia Corporate CA
Subject DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Corporate CA
Not Before	YYMMDDHHMMSS (Key Ceremony date)
Not After	YYMMDDHHMMSS (Key Ceremony date) + 10y 1m
Validity	10y 1m
Key Specification	RSA 3072
Signature Algorithm	SHA256WithRSA

TnTrust Qualified Corporate CA	
Issuer DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia Corporate CA
Subject DN	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Qualified Corporate CA
Not Before	YYMMDDHHMMSS (Key Ceremony date)
Not After	YYMMDDHHMMSS (Key Ceremony date) + 10y 1m
Validity	10y 1m
Key Specification	RSA 3072
Signature Algorithm	SHA256WithRSA

The common extensions of the TN PKI CAs are described in the table below:

Extension	Values	Critical
Tunisian National Root CA		
basic Constraints	CA: TRUE	Yes
key Usage	Certificate Sign, CRL Sign	Yes
Subject Key Identifier	Public key hash value of the certificate.	
Authority Key Identifier	Public key hash value of the issuer certificate.	
Certificate Policies	not included in Root CA certificate	
CRL Distribution Points	not included in Root CA certificate	
Tunisia Gov CA		
basic Constraints	CA:TRUE	Yes
key Usage	Certificate Sign, CRL Sign	Yes
Subject Key Identifier	Public key hash value of the certificate.	
Authority Key Identifier	Public key hash value of the issuer certificate.	
Certificate Policies	2.16.788.1.2.6.1.9	
CRL Distribution Points	http://crl.certification.tn/tunrootca.crl	
Tunisia Corporate CA		
basic Constraints	CA:TRUE	Yes
key Usage	Certificate Sign, CRL Sign	Yes
Subject Key Identifier	Public key hash value of the certificate.	
Authority Key Identifier	Public key hash value of the issuer certificate.	

Certificate Policies	2.16.788.1.2.6.1.9	
CRL Distribution Points	http://crl.certification.tn/tunrootca.crl	
TnTrust Gov CA		
basic Constraints	CA:TRUE, pathlen: 0	Yes
key Usage	Certificate Sign, CRL Sign	Yes
Subject Key Identifier	Public key hash value of the certificate.	
Authority Key Identifier	Public key hash value of the issuer certificate.	
Certificate Policies	2.16.788.1.2.6.1.9	
CRL Distribution Points	http://crl.certification.tn/ tunisiagovca.crl	
TnTrust Qualified Gov CA		
basic Constraints	CA:TRUE, pathlen: 0	Yes
key Usage	Certificate Sign, CRL Sign	Yes
Subject Key Identifier	Public key hash value of the certificate.	
Authority Key Identifier	Public key hash value of the issuer certificate.	
Certificate Policies	2.16.788.1.2.6.1.10	
CRL Distribution Points	http://crl.certification.tn/ tunisiagovca.crl	
TnTrust Corporate CA		
basic Constraints	CA:TRUE, pathlen: 0	
key Usage	Certificate Sign, CRL Sign	
Subject Key Identifier	Public key hash value of the certificate.	
Authority Key Identifier	Public key hash value of the issuer certificate.	
Certificate Policies	2.16.788.1.2.6.1.9	
CRL Distribution Points	http://www.certification.tn/tunisiacorporateca.crl	
TnTrust Qualified Corporate CA		
basic Constraints	CA:TRUE, pathlen: 0	Yes
key Usage	Certificate Sign, CRL Sign	Yes
Subject Key Identifier	Public key hash value of the certificate.	
Authority Key Identifier	Public key hash value of the issuer certificate.	
Certificate Policies	2.16.788.1.2.6.1.10	
CRL Distribution Points	http://www.certification.tn/tunisiacorporateca.crl	

7.1.2.2 Extensions of end-user

The common extensions of the end-user certificates are described in the tables below:

a) OV SSL certificates :

Extension Name	Critical	Description
Authority Key Identifier	No	Public key hash value of the issuer certificate
Subject Key Identifier	No	Public key hash value of the certificate.
Key Usage	No	Signing, key encipherment, data encipherment, and key agreement fields are set
Certificate Policies	No	Policy Identifier OID: 2.16.788.1.2.6.1.9.1.1 (for governmental entities) or 2.16.788.1.2.6.1.9.2.1 (for corporate entities) Policy Qualifier Info – CPS: https://www.certification.tn/cps
Basic Contraints	No	CA : FALSE
Subject Alternative Name	No	May contain alternative domain names of the subject.
CRL Distribution Points	No	HTTP URL of the CRL signed by the CA issuer certificate.
Authority Information Access	No	Addresses of the issuer certificate and the OCSP service.
Extended Key Usage	No	Server authentication and client authentication values are set.

b) OV Wildcard SSL certificates:

Extension Name	Critical	Description
Authority Key Identifier	No	Public key hash value of the issuer certificate
Subject Key Identifier	No	Public key hash value of the certificate.
Key Usage	Yes	Digital Signature, key Encipherment are set

Certificate Policies	No	Policy Identifier OID: 2.16.788.1.2.6.1.9.1.1 (for governmental entities) or 2.16.788.1.2.6.1.9.2.1 (for corporate entities) Policy Qualifier Info – CPS: https://www.certification.tn/cps
Basic Contraints	No	CA : FALSE
Subject Alternative Name	No	Same wildcard FQDN as in the Subject CN field
CRL Distribution Points	No	HTTP URL of the CRL signed by the issuer certificate.
Authority Information Access	No	Addresses of the issuer certificate and the OCSP service.
Extended Key Usage	No	Server authentication and client authentication values are set.

c) EV SSL certificates:

Extension Name	**Critical**	**Description**
Authority Key Identifier	No	Public key hash value of the issuer certificate
Subject Key Identifier	No	Public key hash value of the certificate.
Key Usage	No	Signing, key encipherment, data encipherment, and key agreement fields are set
Certificate Policies	No	Policy Identifier OID: 2.16.788.1.2.6.1.9.1.2 (for governmental entities) or 2.16.788.1.2.6.1.9.2.2 (for corporate entities) Policy Qualifier Info – CPS: https://www.certification.tn/cps
Basic Contraints	No	CA : FALSE
Subject Alternative Name	No	May contain alternative

		domain names of the subject.
CRL Distribution Points	No	HTTP URL of the CRL signed by the issuer certificate.
Authority Information Access	No	Addresses of the issuer certificate and the OCSP service.
Extended Key Usage	No	Server authentication and client authentication values are set.

d) Qualified signature certificates:

Extension Name	**Critical**	**Description**
Authority Key Identifier	No	Public key hash value of the issuer certificate
Subject Key Identifier	No	Public key hash value of the certificate.
Key Usage	Yes	Digital Signature non Repudiation fields are set
Certificate Policies	No	Policy Identifier OID: 2.16.788.1.2.6.1.10.1.1 (for governmental entities) Or 2.16.788.1.2.6.1.10.2.1 (for corporate entities) Policy Qualifier Info – CPS: http://www.certification.tn/pub/pds-tuntrustgovca.pdf Or Policy Qualifier Info – CPS: http://www.certification.tn/pub/pds-tuntrustcorpca.pdf
Basic Contraints	No	CA : FALSE
Subject Alternative Name	No	May contain alternative domain names of the subject.
CRL Distribution Points	No	HTTP URL of the CRL signed by the issuer certificate.
Authority Information	No	Addresses of the issuer certificate and

Access		the OCSP service.
qcStatements	OID : 0.4.0.1862.1.1 (QcCompliance)	not applicable
	OID : 0.4.0.1862.1.2 (QcLimitValue)	not applicable
	OID: 0.4.0.1862.1.4 (QcSSCD)	Fixed http://www.certification.tn/pub/pds-tuntrustgovca.pdf (for governmental entities) or http://www.certification.tn/pub/pds-tuntrustcorpca.pdf (for corporate entities)
Extended Key Usage	No	Email protection

e) Authentication certificates:

Extension Name	**Critical**	**Description**
Authority Key Identifier	No	Public key hash value of the issuer certificate
Subject Key Identifier	No	Public key hash value of the certificate.
Key Usage	Yes	Key Enciphrment
Certificate Policies	No	Policy Identifier OID: 2.16.788.1.2.6.1.9.1.5 (for governmental entities) or 2.16.788.1.2.6.1.9.2.5 (for corporate entities) Policy Qualifier Info – CPS: https://www.certification.tn/cps
Basic Contraints	No	CA : FALSE
Subject Alternative Name	No	May contain alternative domain names of the subject.
CRL Distribution Points	No	HTTP URL of the CRL signed by the issuer certificate.
Authority Information Access	No	Addresses of the issuer certificate and the OCSP service.
Extended Key Usage	No	Client authentication

		Smart Card Logon.

f) OV Code Signing certificates:

Extension Name	Critical	Description
Authority Key Identifier	No	Public key hash value of the issuer certificate
Subject Key Identifier	No	Public key hash value of the certificate.
Key Usage	Yes	Digital Signature
Certificate Policies	No	Policy Identifier OID: 2.16.788.1.2.6.1.9.1.3 (for governmental entities) or 2.16.788.1.2.6.1.9.2.3 (for corporate entities) Policy Qualifier Info – CPS: https://www.certification.tn/cps
Basic Contraints	No	CA : FALSE
Subject Alternative Name	No	May contain alternative domain names of the subject.
CRL Distribution Points	No	HTTP URL of the CRL signed by the issuer certificate.
Authority Information Access	No	Addresses of the issuer certificate and the OCSP service.
Extended Key Usage	Yes	Code Signing

g) EV Code Signing certificates:

Extension Name	Critical	Description
Authority Key Identifier	No	Public key hash value of the issuer certificate
Subject Key Identifier	No	Public key hash value of the certificate.
Key Usage	Yes	Digital Signature
Certificate Policies	No	Policy Identifier OID: 2.16.788.1.2.6.1.9.1.4 (for governmental entities) or 2.16.788.1.2.6.1.9.2.4 for corporate entities) Policy Qualifier Info – CPS:

		https://www.certification.tn/cps
Basic Contraints	No	CA : FALSE
Subject Alternative Name	No	May contain alternative domain names of the subject.
CRL Distribution Points	No	HTTP URL of the CRL signed by the issuer certificate.
Authority Information Access	No	Addresses of the issuer certificate and the OCSP service.
Extended Key Usage	Yes	Code Signing

7.1.3 Algorithm object identifiers

The algorithms with OIDs supported by this CA and its subordinates are:

Algorithm	Object Identifier
SHA2withRSAEncryption	1.2.840.113549.1.1.13
rsaEncryption	1.2.840.113549.1.1.1

7.1.4 Name forms

Certificates issued by the subsidiaries of this CA contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields. Distinguished names are in the form of an X.501 printable string.

7.1.5 Name constraints

Not implemented.

7.1.6 Certificate policy object identifier

Each certificate references a policy OID, and may contain several as long as none of the policy constraints conflict.

For information see section 7.1.2 of this document.

7.1.7 Usage of Policy Constraints extension

Not implemented.

7.1.8 Policy qualifiers syntax and semantics

The subsidiaries of this CA do not currently issue certificates with policy qualifiers.

7.1.9 Processing semantics for the critical Certificate Policies extension

PKI client applications process extensions marked as critical.

7.2 CRL profile

The Tunisian National Root CA and its subordinates issue X.509 Version 2 CRLs in accordance with IETF PKIX RFC 5280.

The intermediate CAs, issuing CAs and end user Subscriber Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE.

Field	Value
Version	V2 in accordance with RFC 5280.
Issuer DN	The Entity who has signed and issued the CRL
Effective date	Issue date of the CRL. CRLs are effective upon issuance.
Next update	Date by which the next CRL will be issued.
Signature Algorithm	Object identifier of the algorithm used to sign the certificate sha256RSA.
Authority Key Identifier	Populated by CA application contains key id (SHA1) of issuer public key
CRL Number	A monotonically increasing sequence number in accordance with RFC 5280
This update	Issuance
Next update	Date of Issuance + <*number of day validity*>

7.3 OCSP profile

The TN PKI OCSP functionality is built according to RFC 6960.

The TN PKI provides uninterrupted on-line certificate status protocol OCSP support which is a real time certificate status inquiry. By this service, when appropriate certificate status inquiries are received, the status of certificates and additional information as required by the protocol are returned to the inquirer as the response.

7.3.1 Version Number

The OCSP service provided by TN PKI supports the v1 protocol version under the "IETF RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP" document.

7.3.2 OCSP Extension

In the content of OCSP service provided by TN PKI, extensions defined in RFC 6960 may be used when necessary. However, it is not mandatory to use all extensions other than the basic OCSP information.

7.4 Time Stamping Profile for Time Stamping Services

The TN PKI CAs maintain a record of the Time Stamping profile it uses in an independent technical document.

This will be made available at the discretion of the TN PKI, on request from parties explaining their interest.

The common extensions of the time-stamping certificates are described in the tables below:

Extension Name	**Critical**	**Description**
Authority Key Identifier	No	Public key hash value of the issuer certificate
Subject Key Identifier	No	Public key hash value of the certificate.
Key Usage	No	Digital Signature
Certificate Policies	No	Policy Identifier OID: 2.16.788.1.2.6.1.11 Policy Qualifier Info – CPS: https://www.certification.tn/cps
Basic Contraints	No	CA : FALSE
Subject Alternative Name	No	May contain alternative domain names of the subject.
CRL Distribution Points	No	HTTP URL of the CRL signed by the issuer certificate.
Authority Information Access	No	Addresses of the issuer certificate and the OCSP service.
Extended Key Usage	Yes	Time Stamping (2.3.6.1.5.5.7.3.8)

8 Compliance Audit and Other Assessments

The terms and conditions of this CP/CPS and all dependent rules and regulations will be used to conduct compliance audits for:

- The Tunisian National Root CA and its subsidiaries
- The TN PKI RA

8.1 Frequency or circumstances of assessment

An annual audit is performed by an independent external auditor to assess the National Digital Certification Agency's compliance with CA WebTrust/ETSI .

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.

8.2 Identity/qualifications of assessor

The National Digital Certification Agency‘s CAs compliance audits are performed by a public accounting firm that:

- Demonstrates proficiency in conducting the WebTrust/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.

8.3 Assessor's relationship to assessed entity

The National Digital Certification Agency has selected an auditor/assessor who is completely independent from it.

8.4 Topics covered by assessment

The scope of the annual audit for Certification Authorities examination includes:

- CA business practices disclosure,
- CA environmental controls,
- CA key life cycle management, and
- Certificate life cycle management.

8.5 Actions taken as a result of deficiency

With respect to compliance audits of TN PKI's operations, significant exceptions or deficiencies identified during the compliance audit will result in a determination of actions to be taken. This determination is made by TN PKI management with input from the auditor. If exceptions or deficiencies are identified, TN PKI management is responsible for developing and implementing a corrective action plan. If TN PKI determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the PKI, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, TN PKI management will evaluate the significance of such issues and determine the appropriate course of action.

8.6 Communication of results

The audit results of processes that are audited according to the ETSI EN 319 411-1 and ETSI EN 319 411-2 standards are communicated officially to TN PKI by the auditing body.

The results of the internal audit are included in the internal audit reports and submitted to evaluation by the relevant authorized persons.

The NDCA makes its Audit Report publicly available no later than three months after the end of the audit period.

9 Other Business and Legal Matters

9.1 Fees

The National Digital Certification Agency provides a price list for certification and registration services on the website www.certification.tn.

9.1.1 Certificate issuance or renewal fees

The National Digital Certification Agency can charge fees for issuing certificates according to the respective price list published on their website or made available upon request.

The update of the fees goes through the board of the NDCA. After a favorable opinion, the NDCA forward the proposal to the Ministry for approval.

Before the implementation of the new fees, the NDCA commits to notify its customers and partners in a period of time of at least one month of the effective date of these new fees.

9.1.2 Certificate access fees

Access to the certificates is not the subject of particular billing from NDCA.

9.1.3 Revocation or status information access fees

There is no charge for certificate revocation and the provision of certificate status information.

9.1.4 Fees for other services

The National Digital Certification Agency may charge for other additional services such as timestamping.

9.1.5 Refund Policy

The NDCA does not refund the fees of certificates because the acceptance of any certificate request is done only if all the paperwork is in order. An incomplete application is automatically rejected.

9.2 Financial responsibility

9.2.1 Insurance coverage

This CP / CPS made no special requirements for a specific insurance underwriting.

9.2.2 Other assets

No Stipulation.

9.2.3 Insurance or warranty coverage for end-entities

Not applicable.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Any information or data the National digital certification Agency obtains in the course of business transactions is considered confidential, except for information defined in section 9.3.2. This includes, but is not limited to business plans, sales information, trade secrets, organizational names, registration information, and subscriber data.

9.3.2 Information not within the scope of confidential information

Any information that is already publicly available is not considered confidential, nor is any information considered confidential which TN PKI is explicitly authorized to disclose (e.g. by written consent of involved party, by law or because it is part of the publicly available certificate information).

9.3.3 Responsibility to protect confidential information

The National Digital Certification Agency is responsible to take all required measures to comply with the Tunisian Data Protection Law and any other relevant regulations.

9.4 Privacy of personal information

9.4.1 Privacy Plan

The National Digital Certification Agency fully complies with the Tunisian Act on the protection of personal data and other applicable legislation. Information and data can be used where needed for professional handling of the services provided herein.

9.4.2 Information treated as private

Any information about subscribers and requesters that is not made public through the certificates issued by this CA, the CRL, or the LDAP directory’s content is considered private information.

9.4.3 Information not deemed private

Any and all information made public in a certificate issued by this CA, or its CRL, or by a publicly available service is not considered confidential.

9.4.4 Responsibility to protect private information

Participants that receive private information are to secure it from compromise, and refrain from using it or disclosing it to third parties.

9.4.5 Notice and consent to use private information

Unless where otherwise stated in this CP/CPS, the applicable Privacy Policy or by agreement, private information will not be used without the consent of the party to whom that information applies.

9.4.6 Disclosure pursuant to judicial or administrative process

The National Digital Certification Agency will only release or disclose private information on judicial or other authoritative order.

9.4.7 Other information disclosure circumstances

The National Digital Certification Agency will solely disclose information protected by the Tunisian Act on the protection of personal data on judicial or other authoritative order.

9.5 Intellectual property rights

All NDCA intellectual property rights including all trademarks and copyrights of all NDCA's documents remain the sole property of the National Digital Certification Agency.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The National Digital Certification Agency warrants full compliance with all provisions stated in this CP/CPS.

9.6.2 RA representations and warranties

TN PKI RA warrants full compliance with all provisions stated in this CP/CPS, related agreements and documents.

9.6.3 Subscriber representations and warranties

Subscribers warrant full compliance with all provisions stated in this CP/CPS and other related agreements and documentation.

9.6.4 Relying party representations and warranties

Relying parties warrant full compliance with the provisions of this CP/CPS and related agreements.

9.6.5 Representations and warranties of other participants

Any other participant warrants full compliance with the provisions set forth in this CP/CPS and related agreements.

9.7 Disclaimers of warranties

Except for the warranties stated herein including related agreements and to the extent permitted by applicable law, TN PKI disclaims any and all other possible warranties, conditions, or representations (express, implied, oral or written), including any warranty of merchantability or fitness for a particular use.

9.8 Liability

9.8.1 Liability of TN PKI

The National Digital Certification Agency is only liable for damages which are the result of TN PKI's failure to comply with this CP/CPS and which were provoked deliberately or wantonly negligent.

TN PKI 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. TN PKI is not liable for any damages resulting from infringements by the Certificate Holder or the Relying Party on the applicable terms and conditions.

TN PKI is not in any event be liable for damages that result from force major events as detailed in section 9.16.4. TN PKI 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 TN PKI.

9.8.2 Liability of the Certificate Holder

The Certificate Holder is liable to TN PKI 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.

9.9 Indemnities

Not applicable.

9.10 Term and termination

9.10.1 Term

This Certificate Policy and Certification Practice Statement and respective amendments become effective as they are published on the National Digital Certification Agency website at http://www.certification.tn/.

9.10.2 Termination

This CP/CPS will cease to have effect when a new version is published on the NDCA website.

9.10.3 Effect of termination and survival

After termination, the certificate may no longer be used. However, all provisions regarding confidentiality of personal and other data will continue to apply without restriction after termination. Also, the termination is not affect any rights of action or remedy that may have accrued to any of the parties up to and including the date of termination.

9.11 Individual notices and communications with participants

Unless otherwise specified by agreement between the parties, TN PKI Participants use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for amendment

TN PKI will implement changes with little or no impact for subscribers and relying parties to this Certificate Policy & Certificate Practice Statement upon the approval of the board committee of NDCA.

Updated CP/CPS become final and effective by publication on the NDCA website and will supersede all prior versions of this CP/CPS.

9.12.2 Notification mechanism and period

The NDCA board committee can decide to amend this CP/CPS without notification for amendments that are non-material (with little or no impact). The NDCA executive board, at its sole discretion, decides whether amendments have any impact on the subscriber and/or relying parties.

All changes to the CP/CPS will be published according to section 2 of this CP/CPS.

9.12.3 Circumstances under which OID must be changed

No Stipulation.

9.13 Dispute resolution provisions

In case of any dispute or controversy in connection with the performance, execution or interpretation of this CP/CPS, the parties will endeavor to reach amicable settlement.

9.14 Governing law and place of jurisdiction

This CP/CPS is governed, construed and interpreted in accordance with the laws of Tunisia. This choice of law is made to ensure uniform interpretation of this CP/CPS, regardless of the place of residence or place of use of TN PKI Certificates or other products and services. The law of Tunisia applies also to all TN PKI commercial or contractual relationships in which this CP/CPS may apply or quoted implicitly or explicitly in relation to TN PKI products and services where TN PKI acts as a provider, supplier, beneficiary receiver or otherwise.
Each party, including NDCA partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Ariana, Tunisia.

9.15 Compliance with applicable law

This Certificate Policy & Certification Practice Statement and rights or obligations related here to are in accordance with Tunisia Law.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CP/CPS may not be the only document which comprises the agreement between the parties involved. Any other agreements may further restrict this CP/CPS, but no document or agreement may lessen the rules and stipulations of this CP/CPS. Any document which serves as an annex to this CP/CPS are made available to all parties involved.

9.16.2 Assignment

Parties to this CP/CPS may not assign any of their rights or obligations under this CP/CPS or applicable agreements without the written consent of NDCA.

9.16.3 Severability Clause

To the extent permitted by applicable law, TN PKI's Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements contain, severability, survival, merger, and notice clauses. A severability clause in an agreement prevents any determination of the invalidity or unenforceability of a clause in the agreement from impairing the remainder of the agreement. A survival clause specifies the provisions of an agreement that continue in effect despite the termination or expiration of the agreement. A merger clause states that all understandings concerning the subject matter of an agreement are incorporated in the agreement. A notice clause in an agreement sets forth how the parties are to provide notices to each other.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeur

TN PKI is not in default and the customer cannot hold TN PKI responsible and/or liable for any damages that result from (but are not limited to) the following type of events any delay, breach of warranty, or cessation in performance caused by :

a) Acts of God;

b) b) Acts of War;

c) c) Acts of Terrorism;

d) d) Epidemics;

e) e) Power or telecommunication services failure;

f) f) Earthquake;

g) g) Flood;

h) h) Fire; or

i) i) Any other natural or man-made disasters

TN PKI takes commercially reasonable measures to mitigate the effects of force major in duetime.

9.17 Other provisions

No Stipulation.

Appendix A1: Supplemental Validation Procedures for Extended Validation (EV) SSL Certificates

The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) SSL Certificates can be accessed at https://cabforum.org/extended validation/

Appendix A2: Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

1. Root CA Certificates

	Strength of algorithm
Digest algorithm	SHA-256
RSA	4096 bit

2. Subordinate CA Certificates

	Strength of algorithm
Digest algorithm	SHA-256
RSA	4096 bit

3. Issuing CA Certificates

	Strength of algorithm
Digest algorithm	SHA-256
RSA	3072 bit

4. Subscriber Certificates

	Strength of algorithm
Digest algorithm	SHA-256
RSA	2048 bit

Appendix A3: EV Certificates Required Certificate Extensions

1. Root CA Certificate

Root certificates generated after October 2006 MUST be X.509 v3.

a) basicConstraints

If the certificate is v3 and is created after October 2006, this extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The CA field MUST be set true. The *pathLenConstraint* field SHOULD NOT be present.

b) keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for *CertSign* and *cRLSign* MUST be set. All other bit positions SHOULD NOT be set.

c) certificatePolicies

This extension SHOULD NOT be present.

d) extendedKeyUsage

This extension is not present.

All other fields and extensions are set in accordance to RFC 5280.

2. Intermediate CA Certificate

a) certificatePolicies

MUST be present and SHOULD NOT be marked critical. The set of policy identifiers MUST include the identifier for TN PKI's EV policy.

certificatePolicies:policyIdentifier (Required)

- the **anyPolicy** identifier if subordinate CA is controlled by TN PKI

b) cRLDistributionPoint

is always present and NOT marked critical. It contains the HTTP URL of TN PKI's CRL service.

c) authorityInformationAccess

MUST be present and MUST NOT be marked critical.

SHALL contain the HTTP URL of the Issuing CA's OCSP responder. An HTTP accessMethod SHOULD be included for TN PKI's certificate.

d) basicConstraints

This extension MUST be present and MUST be marked critical in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The CA field MUST be set true. The pathLenConstraint field MAY be present.

e) keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for CertSign and cRLSign MUST be set. All other bit positions MUST NOT be set.

All other fields and extensions MUST be set in accordance to RFC 5280.

3. Subscriber Certificate

f) certificatePolicies

MUST be present and SHOULD NOT be marked critical. The set of policyIdentifiers MUST include the identifier for TN PKI's EV policy.

certificatePolicies:policyIdentifier (Required)

- EV policy OID certificatePolicies:policyQualifiers:policyQualifierId (Required)
- id-qt 2 [RFC 5280] CertificatePolicies:policyQualifiers:qualifier (Required)
- URI to the Certificate Practice Statement

g) cRLDistributionPoint

is always present and NOT marked critical. It contains the HTTP URL of TN PKI's CRL service.

h) authorityInformationAccess

is always present and NOT marked critical. SHALL contain the HTTP URL of TN PKI's OCSP responder. An HTTP accessMethod MAY be included for TN PKI's certificate.

i) basicConstraints (optional)

If present, the CA field MUST be set false.

j) keyUsage (optional)

If present, bit positions for CertSign and cRLSign MUST NOT be set.

k) extKeyUsage

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. Other values SHOULD NOT be present.

l) SubjectAltName

populated in accordance with RFC5280 and criticality is set to FALSE. All other fields and extensions set in accordance to RFC 5280.

Appendix B: Supplemental Validation Procedures for Extended Validation (EV) Code-Signing Certificates

The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) Code Signing Certificates can be accessed at https://cabforum.org/ev-code-signing-certificate-guidelines/

Appendix C: Supplemental Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates

The current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates can be accessed at https://cabforum.org/baseline-requirements-documents/