



NATIONAL DIGITAL CERTIFICATION AGENCY  
*www.certification.tn*

## CERTIFICATE POLICY V1.0

# Contents

<b>1</b>	<b>Introduction</b>	<b>8</b>
1.1	Overview	8
1.1.1	Roles of the NDCA CP	8
1.1.2	Compliance with applicable standards	9
1.1.3	Policy overview	9
1.1.4	NDCA services	9
1.2	Identification	10
1.3	Tunisian PKI participants	10
1.3.1	Certification Authority (CA)	10
1.3.2	Registration Authorities (RA)	10
1.3.3	Repositories	11
1.3.4	Subscribers	12
1.3.5	Other participants	12
1.4	Certificate usage	12
1.4.1	Appropriate certificates usage	12
1.4.2	Prohibited certificates usage	12
1.5	Policy administration	12
1.5.1	Organization administering the document	12
1.5.2	Contact person	13
1.5.3	Person determining CP suitability for the policy	13
1.6	Definitions and acronyms	13
<b>2</b>	<b>Publication and Repository Responsibilities</b>	<b>13</b>
2.1	Repositories	13
2.2	Publication of certification information	13
2.3	Time or frequency of publication	14
2.4	Access controls on repositories	14
<b>3</b>	<b>Identification and Authentication (I&amp;A)</b>	<b>14</b>
3.1	Naming	14
3.1.1	Types of names	14
3.1.2	Need of names to be meaningful	14
3.1.3	Anonymity or pseudonymity of subscribers	14
3.1.4	Rules for interpreting various name forms	14

3.1.5	Uniqueness of names . . . . .	14
3.1.6	Recognition, authentication and role of trademarks . . . . .	15
3.2	Initial identity validation . . . . .	15
3.2.1	Method to prove possession of private key . . . . .	15
3.2.2	Authentication of organization identity . . . . .	15
3.2.3	Authentication of individual identity . . . . .	15
3.2.4	Non-verified subscriber information . . . . .	15
3.2.5	Validation of authority . . . . .	15
3.2.6	Criteria for inter-operation . . . . .	16
3.3	Identification and authentication for re-key and renewal requests . . . . .	16
3.4	Identification and authentication for revocation requests . . . . .	16
<b>4</b>	<b>Certificate Life-Cycle Operational Requirements</b>	<b>16</b>
4.1	Certificate application . . . . .	16
4.1.1	Who can submit a certificate application . . . . .	16
4.1.2	Enrollment process and responsibilities . . . . .	16
4.2	Certificate application processing . . . . .	17
4.2.1	Performing identification and authentication functions . . . . .	17
4.2.2	Approval or rejection of certificate applications . . . . .	17
4.2.3	Time to process certificate applications . . . . .	17
4.3	Certificate issuance . . . . .	17
4.3.1	CA actions during certificate issuance . . . . .	17
4.3.2	Notification of subscriber by the CA of issuance of certificate . . . . .	17
4.4	Certificate acceptance . . . . .	17
4.4.1	Conduct for certificate acceptance . . . . .	17
4.4.2	Publication of the certificate by the CA . . . . .	18
4.4.3	Notification of certificate issuance by the CA to other entities . . . . .	18
4.5	Key pair and certificate usage . . . . .	18
4.5.1	Subscribers responsibilities . . . . .	18
4.5.2	Relying party . . . . .	19
4.6	Certificate renewal . . . . .	19
4.6.1	Circumstance for certificate renewal . . . . .	19
4.6.2	Who may request renewal . . . . .	19
4.6.3	Processing certificate renewal requests . . . . .	19
4.7	Certificate re-key . . . . .	19

4.7.1	Circumstance for certificate re-key . . . . .	19
4.7.2	Who may request certification of a new public key . . . . .	20
4.7.3	Processing certificate re-keying requests . . . . .	20
4.8	Certificate Modification . . . . .	20
4.9	Certificate revocation and suspension . . . . .	20
4.9.1	Circumstances for revocation/suspension . . . . .	20
4.9.2	Who can request revocation/suspension . . . . .	21
4.9.3	Procedure for revocation/suspension request . . . . .	21
4.9.4	Revocation/suspension request grace period . . . . .	21
4.9.5	Time within which CA must process the revocation/suspension request . . . . .	21
4.9.6	Revocation/suspension checking requirement for relying parties . . . . .	21
4.9.7	CRL issuance frequency . . . . .	22
4.9.8	Maximum latency for CRLs . . . . .	22
4.9.9	On-line revocation/suspension status checking availability . . . . .	22
4.9.10	On-line revocation checking requirements . . . . .	22
4.9.11	Other forms of revocation/suspension advertisements available . . . . .	22
4.10	Certificate Status Services (CSS) . . . . .	22
4.10.1	Operational characteristics . . . . .	22
4.10.2	Service availability . . . . .	22
4.10.3	Optional features . . . . .	22
4.11	End of subscription . . . . .	22
4.12	Key escrow and recovery . . . . .	23
4.12.1	Key escrow and recovery policy and practices . . . . .	23
4.12.2	Session key encapsulation and recovery policy and practices . . . . .	23
<b>5</b>	<b>Management, Operational, and Physical Controls</b>	<b>23</b>
5.1	Physical security controls . . . . .	23
5.1.1	Site location and construction . . . . .	23
5.1.2	Physical access . . . . .	23
5.1.3	Power and air conditioning . . . . .	24
5.1.4	Water exposures . . . . .	24
5.1.5	Fire prevention and protection . . . . .	24
5.1.6	Media storage . . . . .	24
5.1.7	Waste disposal . . . . .	24
5.1.8	Off-site backup . . . . .	24

5.2	Procedural controls . . . . .	24
5.2.1	Trusted roles . . . . .	24
5.2.2	Number of persons required per task . . . . .	25
5.2.3	Identification and authentication for each role . . . . .	26
5.2.4	Roles requiring separation of duties . . . . .	26
5.3	Personnel controls . . . . .	26
5.3.1	Qualifications, experience, and clearance requirements . . . . .	27
5.3.2	Background check procedure . . . . .	27
5.3.3	Training requirements . . . . .	27
5.3.4	Retraining frequency and requirements . . . . .	27
5.3.5	Job rotation frequency and sequence . . . . .	27
5.3.6	Sanctions for unauthorized actions . . . . .	27
5.3.7	Independent contractor requirements . . . . .	27
5.3.8	Documentation supplied to personnel . . . . .	28
5.4	Audit logging procedures . . . . .	28
5.4.1	Types of event records . . . . .	28
5.4.2	Frequency of processing log . . . . .	28
5.4.3	Retention period for audit log . . . . .	28
5.4.4	Protection of audit log . . . . .	28
5.4.5	Audit log backup procedures . . . . .	28
5.4.6	Audit collection system . . . . .	29
5.4.7	Notification of event-causing subject . . . . .	29
5.4.8	Vulnerability assessments . . . . .	29
5.5	Records archival . . . . .	29
5.5.1	Types of records archived . . . . .	29
5.5.2	Retention period for archive . . . . .	29
5.5.3	Protection of archive . . . . .	29
5.5.4	Archive backup procedures . . . . .	29
5.5.5	Requirements for time-stamping of records . . . . .	30
5.5.6	Archive collection system . . . . .	30
5.5.7	Procedures to obtain and verify archive information . . . . .	30
5.6	Key changeover . . . . .	30
5.7	Compromise and disaster recovery . . . . .	30
5.7.1	Computing resources, software, and/or data are corrupted . . . . .	30
5.7.2	Root CA certificate is revoked . . . . .	31
5.7.3	Entity key is compromised . . . . .	31
5.7.4	Disaster recovery . . . . .	31
5.8	CA or RA termination . . . . .	32

<b>6</b>	<b>Technical Security Controls</b>	<b>32</b>
6.1	Key pair generation and installation	32
6.1.1	Key pair generation	32
6.1.2	Private key delivery to subscriber	32
6.1.3	Public key delivery to certificate issuer	33
6.1.4	CA public key delivery to users	33
6.1.5	CA public key delivery to relying parties	33
6.1.6	Key sizes	33
6.1.7	Public key parameters generation and quality checking	33
6.1.8	Key usage purposes (as per X.509 v3 key usage field)	33
6.2	Private key protection and cryptographic module engineering control	34
6.2.1	Cryptographic module standards and controls	34
6.2.2	Private key (n out of m) multi-person control	34
6.2.3	Private key escrow	34
6.2.4	Private key backup	34
6.2.5	Private key archival	35
6.2.6	Private key transfer into or from a cryptographic module	35
6.2.7	Private key storage on cryptographic module	36
6.2.8	Method of activating private key	36
6.2.9	Method of deactivating private key	36
6.2.10	Method of destroying private key	36
6.2.11	Cryptographic module rating	36
6.3	Other aspects of key pair management	36
6.3.1	Public key archival	36
6.3.2	Certificate operational periods and key pair usage periods	36
6.4	Activation data	37
6.4.1	Activation data generation and installation	37
6.4.2	Activation data protection	37
6.4.3	Other aspects of activation data	37
6.5	Computer security controls	37
6.5.1	Specific computer security technical requirements	37
6.5.2	Computer security rating	37
6.6	Life cycle security controls	37
6.6.1	System development controls	37
6.6.2	Security management controls	37
6.6.3	Life cycle security controls	38
6.7	Network security controls	38
6.8	Time-stamping	38

<b>7</b>	<b>Certificate and CRL Profiles</b>	<b>38</b>
7.1	Certificate profile . . . . .	38
7.1.1	Version number(s) . . . . .	38
7.1.2	Certificate extensions . . . . .	39
7.1.3	Algorithm object identifiers . . . . .	40
7.1.4	Name forms . . . . .	40
7.1.5	Name constraints . . . . .	40
7.1.6	Certificate policy object identifier . . . . .	40
7.1.7	Usage of policy constraints extension . . . . .	40
7.1.8	Policy qualifiers syntax and semantics . . . . .	40
7.1.9	Processing semantics for the critical certificate policies extension . . . . .	40
7.2	CRL profile . . . . .	40
7.2.1	Version number(s) . . . . .	41
7.2.2	CRL and CRL entry extensions . . . . .	41
7.3	OCSP profile . . . . .	41
7.3.1	Version number(s) . . . . .	41
7.3.2	OCSP extensions . . . . .	41
<b>8</b>	<b>Compliance Audit and Other Assessment</b>	<b>41</b>
8.1	Frequency or circumstances of assessment . . . . .	41
8.2	Identity/qualifications of assessor . . . . .	41
8.3	Assessor's relationship to assessed entity . . . . .	41
8.4	Topics covered by assessment . . . . .	42
8.5	Actions taken as a result of deficiency . . . . .	42
8.6	Communication of results . . . . .	42
<b>9</b>	<b>Other Business and Legal Matters</b>	<b>42</b>
9.1	Fees . . . . .	42
9.1.1	Refund policy . . . . .	42
9.2	Financial responsibility . . . . .	42
9.2.1	Insurance coverage . . . . .	42
9.3	Confidentiality of business information . . . . .	42
9.3.1	Scope of confidential information . . . . .	42
9.3.2	Information outside the scope of confidential information . . . . .	43
9.3.3	Responsibility to protect confidential information . . . . .	43
9.4	Privacy of personal information . . . . .	43

9.4.1	Privacy plan . . . . .	43
9.4.2	Information treated as private . . . . .	43
9.4.3	Information not deemed private . . . . .	43
9.4.4	Responsibility to protect private information . . . . .	43
9.4.5	Notice and consent to use private information . . . . .	43
9.4.6	Disclosure pursuant to judicial or administrative process . . . . .	43
9.4.7	Other information disclosure circumstances . . . . .	44
9.5	Intellectual property rights . . . . .	44
9.6	Representations and warranties . . . . .	44
9.7	Disclaimers of warranties . . . . .	44
9.7.1	Limitations of other warranties . . . . .	44
9.7.2	Exclusion of certain elements of damages . . . . .	44
9.8	Limitations of liability . . . . .	44
9.9	Indemnities . . . . .	45
9.10	Term and termination . . . . .	45
9.11	Individual notices and communications with participants . . . . .	45
9.12	Version number and OID management . . . . .	45
9.12.1	Procedure for amendment . . . . .	45
9.12.2	Notification mechanism and period . . . . .	45
9.12.3	Circumstances under which OID must be changed . . . . .	45
9.13	Dispute resolution procedures . . . . .	46
9.14	Governing law . . . . .	46
9.15	Compliance with applicable law . . . . .	46
9.16	Miscellaneous provisions . . . . .	46

# 1 Introduction

NDCA (National Digital Certification Authority) is a Tunisian provider of trusted infrastructure services to web sites, public and private enterprises, electronic commerce service providers, and individuals. Digital certificates and payment services provide the critical web identity and authentication that on-line businesses require to conduct secure e-commerce and communications.

NDCA provides digital certificates for applications through a global public key infrastructure (PKI). This document, called the NDCA CP, covers the NDCA Certificate Policies. The CP is the principal statement of policy governing the national PKI. It sets the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital certificates and providing associated trust services. The authors of this document comprise the members of the Certification Unit (CU). The CU is responsible of managing the National PKI and proposing changes to the CP, updating the document, and soliciting comments on the CP.

The CP, however, does not govern any certification services outside the NDCA. For example, other certification service providers in Tunisia can build their own CP provided that it is compliant with this CP. The NDCA is in charged of verifying its compliance to the Tunisian law via audit operations since it is the root CA.

## 1.1 Overview

### 1.1.1 Roles of the NDCA CP

The CP describes at a general level the overall business, legal, and technical infrastructure. More specifically, it describes:

- appropriate applications for digital certificates and the related assurance levels,
- obligations of Certification Authorities, Registration Authorities, Subscribers and other Certification Service Providers,
- legal matters that must be covered in NDCA Subscriber Agreements and Certification Service Providers Agreements,
- requirements for audit and related security and practices reviews,
- methods to confirm the identity of certificate applicants,
- operational procedures for certificate life cycle services: certificate applications, issuance, acceptance, revocation, and renewal,
- operational security procedures for audit logging, records retention, and disaster recovery,
- physical, personnel, key management, and logical security,
- certificate and Certificate Revocation List content, and
- administration of the CP, including methods of its update.

### 1.1.2 Compliance with applicable standards

The structure of this CP generally corresponds to the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, known as RFC 3647 of the Internet Engineering Task Force (IETF), an Internet standards body. This CP conforms to the RFC 3674 framework in order to make policy mapping and comparisons, assessment, and inter-operation easier for persons using certification services.

### 1.1.3 Policy overview

According to the Tunisian law and related decrees, NDCA provides four categories of certificates. They are issued to individuals, organizations, and certification service providers.

The individual certificates may be used for digital signatures, encryption or access control as proof of identity. They provide assurances of the identity of the subscriber based on his personal (physical) presence and other identification credential.

The organizational certificates are issued to devices to provide authentication; data integrity; and encryption. They provide assurances of the identity of the subscriber based on a confirmation that:

- the Subscriber organization does in fact exist,
- that the organization has authorized the Certificate Application, and
- that the person submitting the Certificate Application on behalf of the Subscriber was authorized to do so.

The certification service provider certificates are issued to an organization for use by a duly authorized representative.

### 1.1.4 NDCA services

The NDCA offers a series of services to assist in the deployment, management, and uses of certificates. NDCA PKI allows enterprises and certification service providers to provide certificates to individuals as well as devices (servers, routers, and firewalls).

NDCA PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and e-commerce applications that are compliant to the law. Certificates and keys supplied by the NDCA ensure high level of security for the exchanged electronic messages.

The individual certificates define two categories of certificates:

- Personal certificates: delivered to individuals for personnel use.
- Enterprise certificates: delivered to the employees to be used for business purposes.

Depending on the certificate purpose, NDCA offers for each of the above mentioned categories two types of usage:

- Digital signature (authentication, non repudiation and integrity).
- Encryption (confidentiality).

Besides, organizational certificates are divided into two types:

- **Web Server Certificates:** these certificates enhance the security of electronic payment operations and remote consulting of confidential data.
- **Network Certificates:** these certificates guarantee the confidentiality and the integrity of exchanged data via secure tunnels and ensures peers authentication.

NDCA is empowered to supply authorizations of VPN use through the Tunisian networks. Moreover, NDCA is able to offer time-stamping services by certifying the date on which a digital signature operation was performed.

## **1.2 Identification**

### **1.3 Tunisian PKI participants**

#### **1.3.1 Certification Authority (CA)**

A CA is an organization that issues digital certificates used in the public domain or within a business or transaction context. NDCA is the Root certification authority in Tunisia. It is also responsible to publish a CPS that includes reference to this CP.

To provide notice to certification service provider and subscribers associated with issued, revoked and suspended certificates, NDCA ensures an appropriate publication in a certificate revocation list and a national certificate repository (LDAP).

The CA shall ensure that all RAs operating on its behalf shall comply with the relevant provisions of this CP concerning the operation of RAs. If no RAs are appointed, the CA is in charged of their obligations. CA personnel associated with PKI roles must be individually responsible for actions they perform.

A CA must:

- issue a CPS that outlines the technical, procedural and personnel policies and practices of the CA and that meets the requirements of all the CPs supported by the CA,
- maintain a CA Repository,
- have in place mechanisms and procedures to ensure that its RAs and subscribers are aware of, and agree with the stipulations in this CP that apply to them,
- establish that any subordinate CA (certification service provider) complies with the CP that is mutually recognized, and
- take all reasonable measures to ensure that subscribers are aware of their respective rights and obligations.

#### **1.3.2 Registration Authorities (RA)**

Any RA operating in compliance with this CP is responsible for all duties assigned to it by the CA. Such parties interact with both the subscriber and the CA to deliver public PKI services to the end user. Roles of NDCA RAs are as follows:

- accept, evaluate, approve or reject the registration of digital certificates,
- register subscribers to NDCA certification services,
- attend all stages of the identification of subscribers as assigned by NDCA according to the type of certificate,
- use official documents to evaluate a subscriber application,
- notifying the CA to issue a certification once the approval of a subscriber application is performed,
- initiate the process to revoke/suspend a certificate and request a certificate revocation/suspension from the NDCA.

RAs obligations include the following points:

- RAs must not issue certificates.
- Each RA is appointed by the CA to perform some of the duties of the CA. Then, RA must comply with the related provisions of this CP and the CPS of the CA.
- An RA is responsible for informing subscribers of all relevant information regarding the rights and obligations of the CA, RA and subscriber contained in this CP, the subscriber agreement, and any other document outlining the terms and conditions of certificate use.
- Records of all actions carried out to perform RA duties must identify the responsible of a particular duty.
- An RA must notify a subscriber of the issuance or the revocation of a certificate.
- When an RA submits subscriber information to a CA, it must certify to the CA that it has verified such information.
- Each person involved in RA duties must ensure that private keys and activation data used to access and operate RA applications are protected.

### 1.3.3 Repositories

NDCA must ensure that there is a certificate repository and an associated Certificate Status Service (CSS). A CSS consists of an up to date CRL and an optional On-line Certificate Status Service (OCSS). These repositories and services shall comply with current standards as stated in the CPS.

NDCA publishes all digital certificates it issues in an on-line LDAP repository. This directory must be publicly accessible and 24hours available. Due the sensitivity of the information provided, NDCA defines procedures and security controls related with LDAP functionalities.

In addition, NDCA publishes Certificate Revocation Lists (CRL) on both LDAP directories and Web server. These CRLs are issued and published in frequent intervals (once a month) or within 2 hours after a submission of revocation request.

### **1.3.4 Subscribers**

A CA may issue certificates to public entities including individuals and/or legal persons (companies). Subscribers are parties that:

- apply for a certificate,
- are identified in a certificate, and
- hold the private key corresponding to the public key that is listed in an end user certificate.

The following is a list of some common subscribers obligations:

- Subscribers should provide complete, accurate and truthful information in their certificate applications.
- Every subscriber must enter into a subscriber agreement, which outlines his/her obligations stating the terms and conditions of use of issued certificates, including permitted applications and purposes.
- The subscriber must fulfill his/her obligations as stated in the subscriber agreement.
- Subscribers must protect their personal private keys, and must take all reasonable measures to prevent their loss, disclosure, modification, or unauthorized use.
- When a subscriber suspects private key compromise, he/she must immediately notify the CA that issued the certificate in a manner specified by that CA.

### **1.3.5 Other participants**

Other participants include providers of certificate service, providers of repository services, and other entities providing PKI-related services.

## **1.4 Certificate usage**

### **1.4.1 Appropriate certificates usage**

NDCA certificates can be used for electronic transactions that support PKI such as e-government, authorization access, on-line administration contents, electronic mail, contracts, accessing web sites and electronic documents archival. Further, they allow internal groups to secure their communications through the use of VPN.

### **1.4.2 Prohibited certificates usage**

The limitations to the usage of NDCA certificates are defined by the key usage (signature or encryption). Furthermore, NDCA test certificates does not provide any assurance regarding the identity of the subscriber.

## **1.5 Policy administration**

### **1.5.1 Organization administering the document**

NDCA is responsible for the registration, maintenance and interpretation of this CP. As a Root CA, it approves other CAs (Certification Service Provider). Such approval is established on the basis of an audit performed on the CP and/or CPS. And as a service provider, NDCA issues certificates to public end entities.

### 1.5.2 Contact person

Address inquiries about the CP to **ance@certification.tn** or to the following address:

**Agence Nationale de Certification Electronique**

**Parc Technologique El Ghazala**

**Route de Raoued Km 3.5 - 2083 Ariana - Tunisie**

### 1.5.3 Person determining CP suitability for the policy

The Certification Unit (CU) is responsible for determining whether this CP and other documents in the nature of Certification Practice Statement (CPS) that supplement or are subordinate to this CP are suitable.

## 1.6 Definitions and acronyms

A list of definitions and acronyms can be found at the end of this CP.

## 2 Publication and Repository Responsibilities

### 2.1 Repositories

NDCA is using its website for publishing CA documents and CRLs, and its CA Repository for publishing certificates and CRLs. As a complement to publishing CRLs in the CA Repository, an OCSS may optionally be offered.

### 2.2 Publication of certification information

NDCA must:

- define a certificate status service,
- issue and update a CRL,
- include the URL of the website containing the CRL within any certificate it issues,
- publish NDCA's CA certificates, certificate service provider related certificate and other certificates in its repository,
- publish the address and other relevant access information for its CSS on the website,
- publish signed CRLs in its repository,
- ensure that CRLs, CA-certificates and other published certificates are publicly available in its repository and,
- ensure that access controls are configured so that only authorized CA personnel can modify its website, repository and CSS.

Personal information collected by a CA and not included in the certificate may not be disclosed without consent of the subscriber unless required by law.

## **2.3 Time or frequency of publication**

NDCA guarantees the publication of newly issued certificates within a maximum delay of one day after their validation.

The publication of the newly issued CRLs must not exceed 2 hours after their generation.

## **2.4 Access controls on repositories**

The NDCA repository shall be available for a high proportion of every 24-hour period. Read only incoming access to LDAP server are permitted.

The authentication of LDAP administrator is done through the use of digital certificates. The data flow between the LDAP administrator and the LDAP server is encrypted (use of SSL).

# **3 Identification and Authentication (I&A)**

## **3.1 Naming**

### **3.1.1 Types of names**

To identify a subscriber, NDCA follows certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names (including a CommonName, LocalityName, StateOrProvinceName, OrganizationName, OrganizationalUnitName, CountryName, StreetAddress) and extended names.

### **3.1.2 Need of names to be meaningful**

The Subject and Issuer names contained in a certificate must be meaningful in the sense that the issuing CA 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**

NDCA does not issue anonymous certificates to subscribers.

### **3.1.4 Rules for interpreting various name forms**

For personal certificates, the Common Name (CN), a Distinguished Name (DN) attribute, contains the legal name as presented in government issued photo-identification.

For server certificates, the CN, a DN attribute, contains the fully qualified domain name of the server. This qualification must be issued by the legal authority that manages domain names.

### **3.1.5 Uniqueness of names**

DNs must be unique among all entities of the Certification Authority of NDCA.

### **3.1.6 Recognition, authentication and role of trademarks**

NDCA does not accept trademarks, logos or otherwise copyrighted graphic or text material for inclusion in its certificates.

## **3.2 Initial identity validation**

### **3.2.1 Method to prove possession of private key**

If the subscriber is responsible for his key pair generation, then the possession of the companion private key for the public key being registered will be proved via the digital signature of the certificate request file.

### **3.2.2 Authentication of organization identity**

The identity of an organization must be authenticated through the following means:

- Consulting the database of a service that identifies organizations or inspecting an organization's articles of incorporation.
- Authenticating the identity of organization or individual based on the documentation or credentials provided.
- Applying additional requirements for applicant organizations such as authorization documents duly signed by authorized personnel.

### **3.2.3 Authentication of individual identity**

The identity of an individual to be the subscriber must be authenticated through the following means:

- Controlling official identity documents.
- Authenticating the identity of organization or individual based on the documentation or credentials provided.
- Requiring physical presence before issuing or delivering a digital certificate.
- Applying additional requirements for applicant organizations such as authorization documents duly signed by authorized personnel.

### **3.2.4 Non-verified subscriber information**

Not applicable.

### **3.2.5 Validation of authority**

NDCA accepts CAs wishing to operate under its hierarchy as Certification Providers. Following an initial approval, audit and signature of an agreement with NDCA, the applicant CA has to provide NDCA with certain identification documents including an authorization letter and an approval decision.

NDCA must validate the identity provided by the applicant CA for the CA certificate generation.

### **3.2.6 Criteria for inter-operation**

Not applicable.

### **3.3 Identification and authentication for re-key and renewal requests**

Certificate re-key means issuance of a new certificate to the subscriber with a generation of a new subscriber's key pair. The request for re-key of a certificate must only be made by the subscriber. The CA must authenticate a request for re-key, and the subscriber must authenticate the subsequent response. A subscriber requesting re-key of a certificate may authenticate the request using the keys corresponding to its valid certificate. When this certificate has expired, changes of subscriber information occur or revocation application was submitted by the subscriber, the request for re-key must be authenticated in the same manner as the initial application of a certificate.

Certificate renewal means issuance of a new certificate to the subscriber without changing the subscriber's key pair or any other information in the certificate. NDCA may renew a certificate to the subscriber if and only if he asks for this service in an explicit manner.

### **3.4 Identification and authentication for revocation requests**

NDCA must authenticate a request for revocation of a certificate. It must establish and make publicly available the process by which it addresses such requests and the means by which it will establish the validity of a request. Requests for revocation of certificates must be logged. NDCA may use an on-line authentication mechanism (digital certificate authentication, PIN, etc.).

## **4 Certificate Life-Cycle Operational Requirements**

For certification providers and subscribers, there is a continuous obligation to inform NDCA of all changes in the information featured in their certificates during its operational period. Other obligations may additionally apply.

### **4.1 Certificate application**

#### **4.1.1 Who can submit a certificate application**

Certificate applicants have the responsibility to provide accurate information on their certificate applications. NDCA requires that the applicant subscriber must be either that individual or his legal representative submits a certificate application.

An application for a certificate, where an organization or an organizational role is the prospective subject, may be made by a prospective subscriber if the signature of the prospective subject is attributable to him.

#### **4.1.2 Enrollment process and responsibilities**

NDCA must ensure that each application is accompanied by:

- proof of the identity of the subscriber,

- when the applicant is not the subscriber, proof of authorization to act on behalf of the subscriber,
- when the applicant is not the subject, proof of authorization that the signature of the subject is attributable to the subscriber,
- proof of authorization for any requested certificate attributes,
- a signed subscriber agreement.

## **4.2 Certificate application processing**

### **4.2.1 Performing identification and authentication functions**

After receiving a certificate application, NDCA may perform identification and authentication procedures to validate the certificate application.

### **4.2.2 Approval or rejection of certificate applications**

Depending on the result of the identification or authentication procedures, NDCA can either approve or reject the certificate application. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

### **4.2.3 Time to process certificate applications**

NDCA must act on and process a certificate application within a time frame of 7 working days once all the necessary documents are provided by the applicant.

## **4.3 Certificate issuance**

### **4.3.1 CA actions during certificate issuance**

The issuance of a certificate indicates a complete and final approval of the certificate application.

Following submission of a certificate application or certificate renewal/re-key request, and verification of the identity of subscribers on the basis of credentials presented, NDCA approves or disapproves the submitted information.

### **4.3.2 Notification of subscriber by the CA of issuance of certificate**

Once the certificate is generated, NDCA notifies the subscriber by a signed electronic mail or an official letter.

## **4.4 Certificate acceptance**

### **4.4.1 Conduct for certificate acceptance**

NDCA must ensure that the subscriber acknowledges acceptance of a certificate and accepts the obligations as articulated in the subscriber agreement.

An issued certificate is deemed accepted by the subscriber when any of the following conditions applies:

- acknowledgment of acceptance by sending an email to [ance@certification.tn](mailto:ance@certification.tn),
- use the certificate for the first time,
- three days lapse from certificate delivery if no feed back is received from the subscriber.

Any objection to accepting an issued certificate must explicitly be notified to NDCA.

#### **4.4.2 Publication of the certificate by the CA**

The CA posts the issued certificates to its LDAP repository once they are accepted by their holders.

#### **4.4.3 Notification of certificate issuance by the CA to other entities**

Once a certificate is generated, the CA sends it to RA.

### **4.5 Key pair and certificate usage**

The responsibilities relating to the use of keys and certificates are described in the following.

#### **4.5.1 Subscribers responsibilities**

Subscribers are responsible for:

- having knowledge on using digital certificates and PKI,
- providing correct and accurate information in their communications with NDCA,
- reading, understanding and agreeing with all terms and conditions in NDCA policies,
- using NDCA certificates for legal and authorized purposes,
- notifying NDCA of any changes in the information submitted,
- ceasing to use NDCA certificate if any featured information becomes invalid,
- ceasing to use NDCA certificate when it becomes invalid,
- when invalid, remove server certificates from any application and/or device they have been installed on,
- preventing the compromise, loss, disclosure, modification, or unauthorized use of their private keys,
- using secure devices or products that provide appropriate protection to their keys,
- requesting the suspension or revocation of a certificate in case of an occurrence that affects the integrity of NDCA certificate.

## 4.5.2 Relying party

The obligations of a relying party are as follows:

- have knowledge on using digital certificates and PKI,
- receive notice of the NDCA's CP and associated conditions for relying parties,
- verify an NDCA certificate by using a CRL in accordance with the certificate path validation procedure,
- trust an NDCA certificate only if all information included in such certificate can be verified successfully,
- rely on NDCA certificates only for appropriate applications in accordance with this CP and with certificate content (e.g., key usage field content).

## 4.6 Certificate renewal

### 4.6.1 Circumstance for certificate renewal

NDCA may issue a new certificate following user authentication using his still valid certificate. If the certificate expires, subscriber must be physically authenticated by a registration authority of NDCA.

Subscribers can use the same key pair up to three times in total, allowing for a total length of three years. Beyond that period, the same key may not be used.

### 4.6.2 Who may request renewal

End-user certificates are renewed by NDCA upon their explicit application.

### 4.6.3 Processing certificate renewal requests

If the certificate to be renewed is still valid, his owner is authenticated through his digital signature. Otherwise authentication procedures are the same as the initial certificate issuance.

The other procedures remain as in the initial certificate issuance including:

- Notification of new certificate issuance to subscriber.
- Conduct constituting acceptance of a renewed certificate.
- Publication of the renewal certificate by the CA.
- Notification of new certificate issuance by the CA to other entities.

If it is still valid, the original certificate must be revoked before issuing the renewal certificate. A new serial number different from the original certificate's must be attributed to the new certificate.

## 4.7 Certificate re-key

### 4.7.1 Circumstance for certificate re-key

NDCA issues a new certificate following user authentication using his still valid certificate. Otherwise, subscriber must be physically authenticated by the registration authority of NDCA.

#### **4.7.2 Who may request certification of a new public key**

End-user certificates and keys are renewed by NDCA upon their explicit application.

#### **4.7.3 Processing certificate re-keying requests**

The other procedures remain as in the initial certificate issuance including:

- Notification of re-key certificate issuance to subscriber.
- Conduct constituting acceptance of a re-key certificate.
- Publication of the new certificate by the CA.
- Notification of new certificate issuance by the CA to other entities.

If it is still valid, the original certificate must be revoked before issuing the re-key certificate. A new serial number different from the original certificate's must be attributed to the new certificate.

### **4.8 Certificate Modification**

Not applicable.

### **4.9 Certificate revocation and suspension**

Suspension, submitted by a subscriber, may last for as long as it is required to establish the conditions that caused the request of suspension. Following negative evidence of such conditions, a subscriber may request the re-activation of a certificate.

NDCA publishes notices of suspended or revoked certificates in its CRL.

#### **4.9.1 Circumstances for revocation/suspension**

NDCA suspends or revokes a digital certificate when:

- There has been a loss, theft, modification, unauthorized disclosure or other compromise of the private key of the certificate.
- The certificate's subject has breached a material obligation under this CP.
- There are computer or communication failure, natural disaster or other cause beyond the person's reasonable control.
- There has been a modification of the information contained in the certificate's subject.

#### **4.9.2 Who can request revocation/suspension**

The revocation/suspension of a certificate may only be requested by:

- the subscriber in whose name the certificate was issued,
- the person who ordered the generation process of the certificate,
- the authorized personnel of the CA or its associated RAs.

The revocation/suspension of a CA-certificate may only be requested by:

- the authorized personnel of the CA on whose behalf the CA-certificate was issued,
- the authorized personnel operating the CA issuing the intermediate CA-certificate.

#### **4.9.3 Procedure for revocation/suspension request**

The origin of any certificate revocation or suspension request must be authenticated before the revocation/suspension is being confirmed.

NDCA must ensure that all additional procedures and requirements with respect to revocation/suspension are set in the CPS. An authenticated revocation/suspension request and any resulting actions taken by the CA, must be recorded and retained. When a certificate is revoked/suspended, full justification for the revocation/suspension must be documented. Besides, the subscriber shall be informed and the revocation/suspension shall be published in the Certificate Status Service (CSS).

#### **4.9.4 Revocation/suspension request grace period**

Once the revocation/suspension request is authenticated, any resulting action must be initiated without delay.

#### **4.9.5 Time within which CA must process the revocation/suspension request**

The time within which CA must process the revocation/suspension request can not exceed two hours beginning from the request reception.

#### **4.9.6 Revocation/suspension checking requirement for relying parties**

Mechanisms available for relying parties to check the status of certificates on which they wish to rely are:

- NDCA website: the newest CRLs are published at [www.certification.tn](http://www.certification.tn)
- NDCA LDAP server: the same CRLs are also available at [ldap.certification.tn](http://ldap.certification.tn)

These two services are available for all users in read only access, during 24 hours a day, seven days a week.

#### **4.9.7 CRL issuance frequency**

Revocation lists of NDCA are updated at every revocation/suspension operation. Otherwise, they are updated frequently with maximum intervals of 30 days.

#### **4.9.8 Maximum latency for CRLs**

Once generated, the new CRL must be immediately posted to the website and to the LDAP server. The revoked/suspended certificate must be immediately removed from the repository.

#### **4.9.9 On-line revocation/suspension status checking availability**

Not applicable.

#### **4.9.10 On-line revocation checking requirements**

Not applicable.

#### **4.9.11 Other forms of revocation/suspension advertisements available**

Not applicable.

### **4.10 Certificate Status Services (CSS)**

#### **4.10.1 Operational characteristics**

The certificate status checking services available to relying parties are the LDAP server and the Web Server of NDCA. To provide correct information, NDCA must ensure that it issues an up to date CRL and that it publishes the newest CRLs within a maximum delay of two hours in the NDCA repository and Website.

The subscriber must check the status of all certificates, before their use, in the certificate validation chain against the current CRLs. He must also verify the authenticity and integrity of CRLs.

#### **4.10.2 Service availability**

The certificate status services provided by NDCA are available 24 hours a day, 7 days a week.

#### **4.10.3 Optional features**

Not applicable.

### **4.11 End of subscription**

Subscriber's subscription ends when a certificate is revoked, expired or the service is terminated.

## **4.12 Key escrow and recovery**

### **4.12.1 Key escrow and recovery policy and practices**

Most often, key escrow systems are established in order to recover private keys used by end-user subscribers for the decryption of encrypted messages that they receive. Ideally, signature keys should not be subject to key escrow. Nonetheless, limitations within end-user software may be unable to support separate keys for signatures and encryption. In such cases, a single key is certified for both digital signature and encryption purposes, and key would be escrowed.

CA and end-user private signing keys shall not be held in a way that provides a backup decryption capability. NDCA shall ensure that private keys remain confidential and maintain their integrity. In particular, NDCA shall ensure that :

- Private keys are backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.
- Private keys are always backed up, stored and recovered in an encrypted format. Furthermore, every private key must be split into two or more parts and placed in different places.
- Where the keys are stored in a hardware module, access controls must take place to ensure that keys are not accessible outside the hardware module.

### **4.12.2 Session key encapsulation and recovery policy and practices**

Not applicable.

## **5 Management, Operational, and Physical Controls**

### **5.1 Physical security controls**

NDCA implements physical controls on its own premises including the following.

#### **5.1.1 Site location and construction**

The CA site contains the hardware and software of the CA, including the CA workstation and any external cryptographic hardware module or token. The physical security controls to manage access to the CA site must be implemented. In addition, the CA site is manually or electronically monitored for intrusion at all times. CA facilities must be located in an area without windows or where windows can be secured effectively.

#### **5.1.2 Physical access**

Physical access is restricted by implementing mechanisms to control access from one area to another or access into high security zones. The CA operations must be performed in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using access control lists and tokens. A site access log shall be kept and inspected periodically. Maintenance and service personnel are escorted and supervised.

### **5.1.3 Power and air conditioning**

The CA facility must be equipped with a non interruptible power supply or generators to ensure a continuous supply of power and air conditioning for a predetermined period of time.

### **5.1.4 Water exposures**

The CA facility must be located such that the systems within are protected from water exposure. The facility may also be able to install equipment that can sense flooding and trigger an alarm.

### **5.1.5 Fire prevention and protection**

The CA facility must be equipped with heat and smoke detectors, alarms, and a fire suppression system appropriate for computer equipment.

### **5.1.6 Media storage**

All removable media and paper containing sensitive encrypted information such as keys for signing certificates and CRLs shall be stored in a secure container. These media are protected from environmental threats such as extreme temperatures. Backup media must be stored in a separate and secure location.

### **5.1.7 Waste disposal**

Information on media used for the storage of information such as keys, activation data, or CA files must be deleted securely or destroyed before released for disposal. The CA can establish procedures for waste disposal of sensitive CA operational data to maintain integrity and confidentiality.

### **5.1.8 Off-site backup**

NDCA must make available a special location for off-site backups and must ensure that facilities used for this purpose, have the same level of security as the primary CA site.

## **5.2 Procedural controls**

### **5.2.1 Trusted roles**

In the Tunisian regulation, three technical tasks must be performed by the certification provider. Thus, NDCA defines the trusted roles described below.

#### **5.2.1.1 CA trusted roles**

NDCA must ensure a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection.

NDCA should provide for a minimum of three distinct CA personnel roles, distinguishing between day-to-day operation, administration of the CA system and the management and audit of those operations.

CA Security Officer (CASO) role includes:

- assigning security privileges and access controls of CA Operators and System Administrators commencement and cessation of CA services,
- review of the audit log to detect CA Operators compliance with system security policy,
- personally conduct or supervise an annual inventory of the CA's records.

CA Operator (CAO) role includes:

- configuring CA security policies,
- verification of CP and CPS compliance,
- creation, renewal or revocation of certificates,
- generating, distributing, and otherwise managing CRLs and OCSS.

CA System Administrator (CASA) role includes:

- configuration and maintenance of the CA system hardware and software,
- creating emergency system restart media to recover from catastrophic system loss,
- performing system backups, software upgrades and recovery, including the secure storage and distribution of the backups and upgrades to an off-site location.

Only these personnel should have access to the hardware and software that control the CA operation.

#### 5.2.1.2 RA trusted roles

NDCA must ensure that RA personnel understand their responsibility for the identification and authentication of prospective subscribers and perform the following functions:

- Acceptance of requests for certificates, certificate change, and revocation.
- Authentication of an applicant's identity and authorizations.
- Transmission of applicant information to the CA.

#### 5.2.2 Number of persons required per task

NDCA applies rigorous control procedures to ensure separation of duties according to job responsibilities. The most sensitive tasks require multiple trusted persons. These control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to sensitive resources. The table below enumerates some examples of sensitive tasks and the minimum number of persons required for each task.

Task	Minimum number of persons required
Processing the subscriber's private key (generation, recovery, delivery, format modification, revocation)	two persons (split-knowledge technique)
Processing to the root CA private key (generation, recovery, delivery, format modification, revocation)	three persons (split-knowledge technique)
Physical access to the CA location site	two persons

### 5.2.3 Identification and authentication for each role

All CA personnel must have their identity and authorization verified before they are:

- included in the access list for the CA site,
- included in the access list for physical access to the CA system,
- given a certificate for the performance of their CA role,
- given an account on the CA system.

Each of these certificates and accounts (with the exception of CA signing certificates) must:

- be directly attributed to an individual,
- be not shared,
- be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls.

CA operations must be secured, using mechanisms such as token-based strong authentication and encryption, when accessed across a shared network.

### 5.2.4 Roles requiring separation of duties

NDCA designates different individuals to fill each of the three roles described above and, at least, one individual shall be appointed per task. For example, CASAs have full control over the CA server and software, but not over the cryptographic relevant information like the private key of the CA. A CASA may not be an CAO or auditor. CAO can manage all certificates, request, profiles and a subset of certificate authorities described by the operator access rules but may not configure the CA or be an CASA. CASOs have full control over the network access to all the server systems of the PKI and may not be CASA, CAO, CASO or auditor. Auditors have read-only access to all components of the PKI to verify that the operation complies with the rules and regulations of this CP. An auditor may not be a CASA, CAO or CASO. Registration authority operators (RAO) can manage a subset of certificates and requests described by the RA policies and the operator access rules. An RAO may not be an CASA, CAO or CASO.

## 5.3 Personnel controls

NDCA must ensure that all personnel performing duties with respect to the operation of a CA or RA must:

- be appointed in writing,
- be bound by contract or statute to the terms and conditions of the position they are to fill,
- have received comprehensive training with respect to the duties they are to perform,
- be bound by statute or contract not to disclose sensitive CA security-relevant information or subscriber information,
- and be not assigned duties that may cause a conflict of interest with their CA or RA duties.

### **5.3.1 Qualifications, experience, and clearance requirements**

The CAO role, which involves creating and managing certificate and key information, is a critical role for the security. The individual assuming this role should be of unquestionable loyalty, trustworthiness and integrity, and should have demonstrated a security consciousness and awareness in his or her daily activities.

All NDCA personnel in sensitive positions shall not as far known have been previously relieved of a past assignment for reasons of negligence or non-performance of duties. NDCA may also specify special requirements that shall be stated in the applicable CPS.

### **5.3.2 Background check procedure**

NDCA makes the relevant checks to prospective employees by means of status reports issued by a competent authority, third-party statements or self-declarations.

### **5.3.3 Training requirements**

NDCA must ensure that all personnel performing duties with respect to the operation of a CA or RA must receive comprehensive training in:

- the CA/RA security principles and mechanisms,
- all PKI software versions in use on the CA system,
- all PKI duties they are expected to perform, and
- disaster recovery and business continuity plans.

### **5.3.4 Retraining frequency and requirements**

Periodic training updates might also be performed to establish continuity and updates in the knowledge of the personnel and procedures.

### **5.3.5 Job rotation frequency and sequence**

Job rotation is mandatory for the trusted roles defined within the framework of certification activities. The maximum period for job rotation can not exceed one year.

### **5.3.6 Sanctions for unauthorized actions**

Appropriate disciplinary actions are taken for unauthorized actions or other violations of NDCA's policies and procedures. Disciplinary actions depend on the frequency and severity of the unauthorized actions. In these cases, the NDCA's statute and the Tunisian labor law must be applied.

An example of severe unauthorized action is the violation of any stipulation of this CP.

### **5.3.7 Independent contractor requirements**

Independent contractors or consultants must not be used to fill trusted positions. However, NDCA can ask for judges help to fulfill certain non-exploitation roles.

### 5.3.8 Documentation supplied to personnel

NDCA must make available to its CA and RA personnel, the CPs it supports, its CPS, any specific statutes, policies, procedures or contracts relevant to their position and to the tasks they perform. The security policy of NDCA and the security levels of the documents provided must be respected.

## 5.4 Audit logging procedures

### 5.4.1 Types of event records

NDCA records events that include but there not limited to:

- Successful and failed attempts to initialize end-users, remove, enable, disable, update and recover users, their keys and certificates.
- Successful and failed attempts to create, remove, login as, set, reset and change passwords of, create, update and recover keys and certificates for the roles within the PKI operating authority.
- Interactions with the certificate repository, including successful and failed connection attempts, read and write operations of the PKI application.
- All events related to certificate revocation, security policy modification and validation, PKI application startup and stop, database backup, cross-certification, certificate and certificate chain validation, database and audit trail management, certificate life-cycle management.
- PKI key generation, storage, retrieval, activation, deactivation, archival and destruction.
- Physical access to the PKI locations.

### 5.4.2 Frequency of processing log

Audit logs are examined at least **once a week** for significant security and operational events as well as statistics establishment. In addition, NDCA reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within its CA and RA systems.

### 5.4.3 Retention period for audit log

Audit logs are retained on-site during **two months** after processing and then archived during three years.

### 5.4.4 Protection of audit log

Electronic and manual audit log files are protected from unauthorized viewing, modification, deletion, or other tampering through the use of physical and logical access controls.

### 5.4.5 Audit log backup procedures

Incremental backups of audit logs are created **weekly** and full backups are performed **every two months**.

#### **5.4.6 Audit collection system**

The audit log collection system must be internal to NDCA.

#### **5.4.7 Notification of event-causing subject**

Subject which caused an audit event to occur are not notified of the audit action.

#### **5.4.8 Vulnerability assessments**

Events in the audit process are logged, in part, to monitor system vulnerability assessments which must be therefore performed, reviewed, and revised.

### **5.5 Records archival**

#### **5.5.1 Types of records archived**

NDCA retains in a trustworthy manner records of the issued digital certificates, audit data, certificate application information and documentation supporting certificate applications.

#### **5.5.2 Retention period for archive**

NDCA retains in a trustworthy manner records of the issued digital certificates for a term of 20 years as specified in the Tunisian law.

#### **5.5.3 Protection of archive**

To protect its archive, only the records administrator may view the archive contents. In addition, the following conditions must be fulfilled:

- Protection against modification of archive.
- Protection against deletion of archive.
- Protection against deterioration of the media on which the archive is stored (exp. requirement for data to be migrated to fresh media).
- Protection against obsolescence of techniques used for archiving.

#### **5.5.4 Archive backup procedures**

The backup procedural scheme includes the following:

- A complete backup should be performed every two months to capture modifications made during that period (issued certificates and CRLs) or once a maximum number of issued certificates is reached.
- A complete annual backup should be performed to capture the overall state of the PKI (configuration files, ...).

- Testing for disaster recovery, which may include testing the process of restoring data from a backup copy, should be performed every six months.
- Sensitive material (such as private keys) should be stored in an encrypted format on all backups.

### **5.5.5 Requirements for time-stamping of records**

Not applicable.

### **5.5.6 Archive collection system**

NDCA archive collection system is internal and therefore should be classified accordingly.

### **5.5.7 Procedures to obtain and verify archive information**

To obtain and verify information, NDCA maintains records under clear hierarchical control and a definite job description.

NDCA retains records in electronic or in paper-based format. NDCA may require applicant for archived data to submit documents in support according to its requirements.

## **5.6 Key changeover**

NDCA key pairs are retired from service at the end of their respective maximum lifetimes. Its issued certificates may be renewed as long as the cumulative certified lifetime of the subordinate CA key pair does not exceed the maximum root CA key pair lifetime. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

Prior to the expiration of the CA Certificate for a Superior CA, key changeover procedures are enacted to facilitate a smooth transition for entities from the old CA key pair to new CA key pair(s). NDCA key changeover process requires that:

- CA ceases to issue new subordinate CA certificates no later than one year before the stop issuance date where the remaining lifetime of the CA key pair equals the approved certificate validity period for the specific type(s) of certificates issued by intermediate CAs in the original CA hierarchy.
- Upon successful validation of subordinate CA (or end-user subscriber) certificate requests received after the stop issuance date will be signed with a new CA key pair.
- The CA continues to issue CRLs signed with the original CA private key until the expiration date of the last certificate issued using the original key pair is reached.

## **5.7 Compromise and disaster recovery**

### **5.7.1 Computing resources, software, and/or data are corrupted**

NDCA must establish business continuity plan that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data.

### 5.7.2 Root CA certificate is revoked

In the event of the need for revocation of a CA's certificate, the following entities must be notified:

- all of its subordinate CAs,
- all CAs with whom it is cross-certified,
- all its subscribers.

NDCA must also:

- publish the certificate serial number in the CSS,
- revoke all certificates signed with the revoked certificate.

After addressing the factors that led to revocation, NDCA may:

- generate a new CA signing key pair,
- re-issue certificates to all subjects whose certificates are revoked,
- ensure that all CSS entries are signed using the new key.

### 5.7.3 Entity key is compromised

In the event of the compromise of a CA's private key, NDCA must:

- revoke the CA-certificates issued to the CA,
- revoke all certificates issued using that key,
- provide appropriate notice.

After addressing the factors that led to key compromise, NDCA must choose whether the following tasks must be performed by NDCA itself or by another certification provider:

- generate a new CA signing key pair,
- generate a new CA certificate,
- after receiving its new certificate, re-issue certificates to all entities and ensure all CSS entries are signed using the new key.

In the event of the compromise, or suspected compromise, of any other entity's private key, the entity must notify NDCA immediately.

### 5.7.4 Disaster recovery

The NDCA's CA must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster.

## 5.8 CA or RA termination

Before terminating its certification activities, NDCA:

- Provides subscribers holding valid certificates within reasonable notice of its intention to cease acting as a CA.
- Revokes all certificates that are still valid at the end of the notice period without seeking subscriber's consent.
- Gives timely notice of revocation to each affected subscriber.
- Makes reasonable arrangements to preserve its records.

## 6 Technical Security Controls

This section deals with the public/private key pair management policy for CAs, RAs, end entities and the corresponding technical controls. It also defines the security measures taken by NDCA to protect its keys and activation data.

### 6.1 Key pair generation and installation

#### 6.1.1 Key pair generation

Within NDCA, key pairs for CAs, RAs and subscribers are generated in such a way that private keys are only known by the authorized users.

NDCA securely generates and protects its own private keys using trustworthy systems. Furthermore, NDCA takes necessary precautions to prevent the compromise or the unauthorized usage of its private keys.

The generation of the key pairs of subscribers can be done in two manners:

- a registration authority in NDCA generates the key pairs of the different subscribers,
- the subscribers generate themselves their key pairs.

In both cases, the generation process must use the approved cryptographic algorithms listed in 7.1.3.

#### 6.1.2 Private key delivery to subscriber

In the case where the keys are not generated by the subscribers, NDCA ensures secure procedures for the delivery of the private keys to their holders.

Thus, within NDCA, access to the hardware and the software modules containing the private keys shall be limited to the authorized personnel. Furthermore, access shall be controlled through the use of electronic access controls and mechanical combination lock sets.

NDCA should maintain the accountability for the location and the state of the modules containing the private keys until their delivery to the subscribers. These ones are physically authenticated. Besides, they shall formally acknowledge the reception of the modules.

### **6.1.3 Public key delivery to certificate issuer**

When the subscribers generate their own key pairs, they should transfer their public keys to an RA from the NDCA in a way ensuring that:

- the public key has not been changed during transit,
- the subscriber possesses the corresponding private key, and
- the subscriber is the legitimate user claimed in the certificate application.

### **6.1.4 CA public key delivery to users**

The certificates containing the public keys of the certification authorities belonging to NDCA should be available to subscribers on the LDAP repositories and on the web server of the NDCA.

### **6.1.5 CA public key delivery to relying parties**

The public key of the root CA should be available to the relying parties on the repositories and the web server of the NDCA.

### **6.1.6 Key sizes**

The size of the key pairs accepted by NDCA shall be sufficiently enough to prevent the determination of the private key, during its period of utilization, using cryptanalysis.

NDCA sets up the following rules for the keys it manages:

- the key pair of the root CA should have a minimum size of 4096 bits,
- the key pairs of the intermediate CAs defined in NDCA and of the certification providers should have a minimum size of 2048 bits,
- the key pairs of the subscribers should have a minimum size of 1024 bits.

### **6.1.7 Public key parameters generation and quality checking**

Not applicable.

### **6.1.8 Key usage purposes (as per X.509 v3 key usage field)**

The use of a specific key is determined by the key usage extension in the X.509 certificate. NDCA distinguishes between:

- the CA signing keys which are the only keys permitted to be used for signing certificates and CRLs, and
- the keys of the subscribers which may be used for authentication, non-repudiation, message integrity and confidentiality.

## 6.2 Private key protection and cryptographic module engineering control

### 6.2.1 Cryptographic module standards and controls

NDCA uses cryptographic modules to ensure the management of the keys it generates. These devices meet the requirements of FIPS PUB 140-1 Level 3 and Level 4. They guarantee, among other things, that any device tampering is immediately detected and that keys cannot leave devices unencrypted.

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

The private keys of the certification authorities defined under NDCA root CA remain under the control of  $n$  out of  $m$  multi-person protection. Therefore NDCA determines a threshold number of persons ( $n$ ) out of a total number of possible persons ( $m$ ) to activate and use a private key of a certification authority.

### 6.2.3 Private key escrow

According to the Tunisian law, NDCA escrows only the subscribers' private keys used for encryption and decryption. However, the subscribers' private keys used for digital signatures or used for access control or authentication are not escrowed. Besides, the private keys of other PKI participants, such as CAs and RAs are not escrowed.

NDCA ensure that the escrow process respects the following criteria:

- It implements the access scheme faithfully and it protects the confidentiality of the information carried (e.g., keys, access requests, etc.).
- It uses mechanisms which maintain and validate the integrity of access requests, responses and stored key data.
- It authenticates the source of the key data and protects the data from disclosure to unauthorized parties.
- It ensures non-repudiation of responses it generates. The escrow process should unambiguously tie the request for access to the returned escrowed data.
- It provides timely access request responses. The response time should meet the needs of the requester.

### 6.2.4 Private key backup

Backup meets a short-term need of business continuity to prevent the loss of functionality due to an accidental loss, corruption, or deletion of the private key. NDCA ensures that the backup of private keys it generates must respond to the following points:

- the choice and the identification of the operating persons who can access or use backed-up keys,
- the security measures that should be taken to protect copies of private keys before their backup,
- the security of the backup medium location,
- the multi-party control to restore the backed-up key material.

The backup of the keys of the intermediate certification authorities should be performed to minimize the risk of key compromise and to ensure continuity of CA operations. NDCA defines the backup process as follows:

- The private keys of the certification authorities are encrypted. The activation data used for encryption should be split into  $m$  portions. These portions are maintained by  $m$  persons such that the presence of  $n$  out of  $m$  persons is sufficient to ensure the recovery of the private key.
- The private keys of the certification authorities are split into  $N$  portions.
- The different splits are exported from the cryptographic module where they are generated into offline supports.
- The supports are kept in locked locations with the highest degree of security.

NDCA presents the backup of the end-entity private keys as a service which is offered to its subscribers. The backup procedure guarantees that end-entity keys are copied and stored in encrypted form. Furthermore, the keys are split and exported from cryptographic modules and they are stored in off-line hardware cryptographic modules.

### **6.2.5 Private key archival**

NDCA ensures an archival service for the private keys of its subordinate certification authorities and those of end-entity used for encryption and decryption. In addition, NDCA offers archives end entity private data upon explicit application of the certificate holders and agreements ( example: private keys used for signature, digital signed documents,...).

NDCA ensures the security of the archival procedure through:

- the determination and the identification of the persons who handle the data during archival,
- the preservation of the same level of security of the archived data during all the period of archive,
- the guarantee of the security of the hardware modules and the locations in which the archived data are kept.

### **6.2.6 Private key transfer into or from a cryptographic module**

Within NDCA, the transfer of private keys into cryptographic modules could take place in the following situations:

- a certification authority generates end-user key pairs on single secured machines. Next, the key pairs are inserted into hardware modules which would be distributed to end-users.
- during the procedures of escrow, backup and archival, a certification authority creates copies of the private keys. Then, it stores the backup copies into cryptographic modules.
- it may be necessary, in case of defection, to move a private key from one cryptographic module to another.

NDCA ensures that all private keys are handled in encrypted forms when they are inserted or extracted from the cryptographic modules. In addition, when it is a matter of certification authorities private keys, NDCA guarantees that the private keys should be split prior to being entered into a series of cryptographic modules. Consequently, only an encrypted portion of the private key is entered into a given cryptographic module in any instance.

### **6.2.7 Private key storage on cryptographic module**

Private keys generated within NDCA should be encrypted when they are stored in cryptographic modules. Furthermore, the certification authorities private keys should be also split.

### **6.2.8 Method of activating private key**

NDCA presents two ways to activate the private keys it generates:

- the certification authorities private keys are activated only by the presence of  $n$  out of  $m$  persons who hold the portions of the private keys pass-phrases,
- the end-users private keys can be activated only by the person holding the relevant pass-phrases. This person is strictly defined by the procedures established within NDCA.

Furthermore, NDCA sets up physical access controls on the machines and the modules holding the private keys.

### **6.2.9 Method of deactivating private key**

After operating on private keys, the NDCA personnel ensure that there is no residual information remaining on the used systems which can conclude an unauthorized recovery of private data. NDCA adopts the following measures:

- overwrite the memory in which the private key was stored prior to the allocation of a new process,
- deactivate the private keys in the following cases: the end of session, the removing of cryptographic modules from their readers, the log off the system and the turn off of the power.

### **6.2.10 Method of destroying private key**

Upon the end of use or the termination of the period of archival, all copies of the private keys defined within NDCA sites are securely destroyed to prevent any possibility of recovery.

### **6.2.11 Cryptographic module rating**

No stipulation.

## **6.3 Other aspects of key pair management**

### **6.3.1 Public key archival**

All public keys generated within NDCA are archived during the periods precised in the Tunisian law.

### **6.3.2 Certificate operational periods and key pair usage periods**

NDCA specifies that the usage periods of the key pairs it generates do not exceed twenty five years for the root certification authority, four years for the intermediate certification authorities and three years for the end-users.

## **6.4 Activation data**

### **6.4.1 Activation data generation and installation**

NDCA ensures that any activation data must be unique and unpredictable. The activation data must have an appropriate level of strength for the keys or data to be protected. In addition, any entity using activation data must have the ability to change them at any time.

### **6.4.2 Activation data protection**

NDCA employs the following controls to protect activation data:

- forbidding users from sharing activation data with unauthorized personnel,
- enforcing multi-person control of CA private keys through splitting the activation data,
- enforcing periodic change of the activation data.

### **6.4.3 Other aspects of activation data**

NDCA securely stores and archives activation data associated with private keys it generates in separate locations.

## **6.5 Computer security controls**

### **6.5.1 Specific computer security technical requirements**

The workstations and servers used in the NDCA systems are configured to provide the minimal functionality required to provide certification and registration services. Furthermore, security controls are used to provide access control and traceability on all transactions and functions affecting the use of the NDCA servers. Detailed logs of these operations are kept to be audited by the specific personnel.

### **6.5.2 Computer security rating**

No stipulation.

## **6.6 Life cycle security controls**

### **6.6.1 System development controls**

Cryptographic modules used within NDCA must be developed using standardized techniques. In addition, they should be tested by the appropriate personnel within NDCA.

### **6.6.2 Security management controls**

The configuration, modification or upgrade of any system within NDCA must be documented and controlled by the security personnel.

### 6.6.3 Life cycle security controls

NDCA performs periodic developments controls and security management controls on its certification systems.

## 6.7 Network security controls

Certification authorities defined within NDCA could never be connected to external networks.

## 6.8 Time-stamping

Not applicable.

# 7 Certificate and CRL Profiles

## 7.1 Certificate profile

All PKI End Entity software must support and correctly process the base (non-extension) X.509 fields and extensions identified in PKIX Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC3280).

At minimum, X.509 certificates generated within NDCA shall contain the following basic fields:

- Version: NDCA issues X.509 Version 3 certificates.
- Serial Number: it must be a unique value per Issuer DN.
- Issuer: X.501 type distinguished name of CA. It is recommended that the organizationName component is included in the name.
- Validity: the first and last date in the validity period for the certificate.
- Subject: X.501 type distinguished name of the certificate holder. It is recommended that the organizationName component is included in the name.
- Subject Public Key Info: the OID (Object Identifier) of the algorithm for the certified public key and the certified public key itself.
- Signature Algorithm: the OID for the algorithm used by the CA to sign the certificate.
- Signature: this field contains the value of the certificate signature.

For specific purposes, NDCA may issue certificates including other basic fields in accordance with the PKIX. The subscriber must claim for other specific basic fields in an explicit manner.

### 7.1.1 Version number(s)

NDCA issues X509 Version 3 certificates, in accordance with the PKIX.

### 7.1.2 Certificate extensions

NDCA issues certificates with the following extensions<sup>1</sup>:

Extension field	Signification	Criticality
Basic Constraints	For both CAs certificates and end users certificates. Its value indicates whether the subject of the certificate is a CA and how deep a certification path may exist through that CA.	C (for CA certificates)
Key usage	For both CAs certificates and end users certificates. The value of this field indicates the authorized usage of the key pair associated to the certificate.	C
Subject Key Identifier	For both CAs certificates and end users certificates. The value of this field is a fingerprint of the Subject Public Key.	NC
Authority Key Identifier	For both CAs certificates and end users certificates. The value of this field is a fingerprint of the Issuer Public Key.	NC
Netscape Cert Type	For both CAs certificates and end users certificates. This field restricts the usage of the certificate to the intended purposes.	NC
Netscape Comment	Only for the end users certificates. This field contains a comment to be displayed in Netscape's comment listbox.	NC
Subject Alternative Name	For both CAs certificates and end users certificates.	NC
Issuer Alternative Name	For both CAs certificates and end users certificates. It's an Alternative Name for the CA: the Email Address.	NC
CRL Distribution Points	For both CAs certificates and end users certificates. This field indicates the URL where a relying party can obtain a CRL to check the certificate's status.	NC

Table 1: Certificate extensions and their criticality

<sup>1</sup>In the criticality column, C stands for *Critical* field and NC indicates a *Non-Critical* one. An application **MUST reject** the certificate if it encounters a *Critical* extension it does not recognize; however, a *Non-Critical* extension **MAY be ignored** if it is not recognized.

### **7.1.3 Algorithm object identifiers**

NDCA must use and end entities must support, for signing and verification, the following algorithms: RSA and SHA-1 (sha1WithRSAEncryption). NDCA only issues certificates for keys for these algorithms.

In addition, NDCA CAs and end entities must support the algorithms approved by PKIX for verification.

### **7.1.4 Name forms**

Each DN must be in the form of an X.501 UTF8String.

### **7.1.5 Name constraints**

No stipulation.

### **7.1.6 Certificate policy object identifier**

No stipulation.

### **7.1.7 Usage of policy constraints extension**

No stipulation.

### **7.1.8 Policy qualifiers syntax and semantics**

No stipulation.

### **7.1.9 Processing semantics for the critical certificate policies extension**

Critical extensions shall be interpreted as defined in PKIX Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC3280).

## **7.2 CRL profile**

All PKI end entity software must support and correctly process the CRL fields and extensions identified in the PKIX.

At minimum, CRLs generated within NDCA shall contain the following basic fields:

- Version: Version of X.509 CRL, version is 2.
- Signature and Signature Algorithm: sha-1WithRSAEncryption shall be used by the CA to sign the CRL.
- Issuer: X.501 type distinguished name of CA. It is recommended that the organizationName component is included in the name.
- Last Update: issue date of the CRL. NDCA CRLs are effective upon issuance.

- Next Update: date by which the next CRL will be issued. CRLs issuance frequency of NDCA CAs is set to 30 days.
- Revoked Certificates: a listing of the revoked certificates, including their serial numbers and revocation date.

### **7.2.1 Version number(s)**

NDCA issues X509 Version 2 CRLs, in accordance with the PKIX.

### **7.2.2 CRL and CRL entry extensions**

Not applicable.

## **7.3 OCSP profile**

Not applicable.

### **7.3.1 Version number(s)**

Not applicable.

### **7.3.2 OCSP extensions**

Not applicable.

## **8 Compliance Audit and Other Assessment**

### **8.1 Frequency or circumstances of assessment**

NDCA is in charged of auditing its subordinate CAs and those of other certificate service providers. This audit can be made periodically or when NDCA decides that after receiving some suspicious information about the security of these certification authorities.

### **8.2 Identity/qualifications of assessor**

Personnel performing audit operations belongs to NDCA and they must be expert in the certification domain. They have to perform the audit following a specific methodology accepted and developed in NDCA.

### **8.3 Assessor's relationship to assessed entity**

The relationship between auditing personnel and the audited entity is a professional relationship. Each entity must perform its duties respecting the limits of its responsibilities.

## **8.4 Topics covered by assessment**

The methodology of audit covers the documents containing details about the architecture of the PKI and the used mechanisms for PKI security. Also, NDCA audit can cover the certification practices and procedures through a personnel audit. Then, NDCA performs a technical audit which covers hardware and software components of the PKI.

## **8.5 Actions taken as a result of deficiency**

NDCA reports systems deficiencies to the audited organization. The correction's actions must be performed according to the agreement between NDCA and the audited organization.

## **8.6 Communication of results**

The audit results can be gathered in reports written by auditors and discussed between the two parties.

# **9 Other Business and Legal Matters**

## **9.1 Fees**

NDCA charges fees for the use of some of its products and services. It publishes a list of the applicable prices. It retains the right to change such fees.

### **9.1.1 Refund policy**

NDCA does not offer refund for all services that it provides.

## **9.2 Financial responsibility**

### **9.2.1 Insurance coverage**

The applicant for an NDCA certificate, which could be used in business transactions, must provide insurance for his transactions.

## **9.3 Confidentiality of business information**

### **9.3.1 Scope of confidential information**

Privacy and confidentiality rules of personal informations are defined by NDCA.

### **9.3.2 Information outside the scope of confidential information**

No information can be considered outside the scope of confidential information without official authorization of NDCA. Such request are accepted in one of the two following cases:

- the party to whom NDCA owes a duty to keep information confidential is the party requesting such information;
- a court order.

NDCA may charge fee to process such disclosure.

### **9.3.3 Responsibility to protect confidential information**

Confidential information are under the NDCA responsibility until they are provided to the authorized parties. The parties reclaiming confidential information have responsibilities to secure these information from compromise and refrain from using or disclosing them to third parties.

## **9.4 Privacy of personal information**

### **9.4.1 Privacy plan**

NDCA process applicant's personal informations according to the Tunisian law.

### **9.4.2 Information treated as private**

Personal information of applicants is treated as private information.

### **9.4.3 Information not deemed private**

Some personal informations including subscriber's certificates are available through NDCA's LDAP repository (ldap.certification.tn).

### **9.4.4 Responsibility to protect private information**

NDCA is responsible of private informations protecting. Its personnel must refrain from using and disclosing them to third parties.

### **9.4.5 Notice and consent to use private information**

Private information of applicants are used by NDCA for issuing certificates. An agreement for confidentiality is signed by applicants, which consent for NDCA to use their private informations.

### **9.4.6 Disclosure pursuant to judicial or administrative process**

When applicants provide their private information to NDCA, verification steps are performed according to the Tunisian law. If an applicant provides false information to NDCA, administrative and judicial processes are applied by the personnel of NDCA.

#### **9.4.7 Other information disclosure circumstances**

No Stipulation.

### **9.5 Intellectual property rights**

NDCA reserves all intellectual property rights associated with its databases, web sites, digital certificates and any other publications including this CP.

### **9.6 Representations and warranties**

The use of NDCA certificates by subscribers and certification service providers is limited by agreements of subscribers, this CP and the related CPS. The participants that may make representations and warranties include CA, RA, subscribers, relying parties.

### **9.7 Disclaimers of warranties**

#### **9.7.1 Limitations of other warranties**

NDCA does not warrant:

- the accuracy of unverifiable pieces of information contained in NDCA certificates.
- the accuracy, authenticity, completeness of any information contained in test or demo certificates.

#### **9.7.2 Exclusion of certain elements of damages**

NDCA is not liable for any damage that occurs when using certificates, including:

- loss of profits,
- loss of data,
- indirect, consequential, damages arising from or in connection with the use, delivery, license, performance or non performance of certificates and digital signatures,
- any other damages except those due to reliance on the verified information in the certificates (test and demo certificates not included),
- liability occurred in any case if the error in verified information is the result of fraud or misconduct of the applicant.

### **9.8 Limitations of liability**

The liability of NDCA is limited by provisions specified for its products and services.

## **9.9 Indemnities**

The subscriber may agree to indemnify and hold NDCA harmless from any act or omission resulting in liability, loss or damage, including reasonable fees that NDCA may incur as a result of:

- any false or misrepresented data supplied by the subscriber.
- any failure to protect the subscriber's private key, to use a trust system as required or to take necessary precautions to prevent the compromise, loss, disclosure, modification or unauthorized use of this private key.
- Breaking any law applicable in the Tunisian country.

## **9.10 Term and termination**

This CP remains used by NDCA until changes will be published and marked by a new version. These changes are applicable **30 days** after publication.

## **9.11 Individual notices and communications with participants**

Individual notices and communications made to NDCA's CA must be addressed to **ance@certification.tn** or by post to:

**Agence Nationale de Certification Electronique**

**Parc Technologique El Ghazala**

**Route de Raoued Km 3.5 - 2083 Ariana -Tunisie**

## **9.12 Version number and OID management**

### **9.12.1 Procedure for amendment**

The assurance level of this CP is indicated by a version number that contains two decimal numbers. The current version is version 1.0.

### **9.12.2 Notification mechanism and period**

Minor changes of this CP does not materially affect the version number. Major changes are notified by publication of this CP in the web site [www.certification.tn](http://www.certification.tn). These changes are applicable 30 days after notification.

### **9.12.3 Circumstances under which OID must be changed**

Minor changes does not affect the CP OID. Major changes that can affect the acceptability of certificates for specific purposes may require the change of the CP OID. NDCA decides for the numbering of versions.

### **9.13 Dispute resolution procedures**

the courts of Ariana are empowered to regulate the litigations.

### **9.14 Governing law**

This CP is governed by the Tunisian law and related decrees and ministry decisions. This law applies also to all commercial or contractual relationships in which this CP may apply.

### **9.15 Compliance with applicable law**

NDCA complies with applicable law in Tunisia. Export of some products and services used in NDCA's PKI may require the approval of government authorities.

### **9.16 Miscellaneous provisions**

Various provisions are applicable in relation with NDCA certificates as found in the Tunisian regulation.

## Definitions

**Activation data** Private data, other than keys, that are required when accessing cryptographic modules.

**CA Certificate** A certificate issued for a CA, that is self-signed or issued by another CA.

**Certificate** A form of credential, which binds an identity to a public key. A certificate will typically contain subjects information including name, the subjects public key, the certificate issuer's name and digital signature, an expiry date and a serial number.

**Certificate Policy (CP)** A set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

**Certificate Revocation List (CRL)** A list signed by a CA that contains the certificates revoked before their expiration date.

**Certification Authority (CA)** A trusted entity that associates a subject with a public and a private key pair. It links the key pair to the subject by issuing a certificate containing the subject public key and information.

**Certification path validation** Process of validating (a) all the digital certificates in a certification path and (b) the required relationships between those certificates, thus validating the contents of the last certificate on the path.

**Certification Practice Statement (CPS)** A statement of the practices a CA employs in issuing and managing certificates.

**Certificate Status Service (CSS)** The service provided through a CRL repository or an OCSS .

**Cross-certification** A certificate issued by one certification authority to a second certification authority so that users of the first certification authority are able to obtain the public key of the second certification authority and verify the certificates it has created. Often cross certification refers specifically to certificates issued to each other by two CAs at the same level in a hierarchy.

**Cryptographic module** The set of hardware, software or a combination of both that implements cryptographic logic or processes, including cryptographic algorithms.

**Decryption** The process of extracting an original message, or plain text, from a cipher text through the application of an appropriate key and algorithm

**Digital signature** A piece of information generated by cryptographic methods, whereby it can be demonstrated that an original message or file has not been deliberately altered or accidentally corrupted, and that the identity of the originator of the file can be authenticated.

**Encryption** The conversion of data into a form that can not be easily understood by unauthorized people. Decryption returns data to its original form.

**End Entity** A Subscriber, Relying Party, or IT-system (that is not a CA or RA) that uses the keys and certificates created within a PKI.

**Entity** An autonomous element within the PKI. This may be a CA, an RA or an End Entity.

**On-line Certificate Status Protocol (OCSP)** A protocol which is used to provide real-time validation of a certificate's status. An OCSP responder is used to respond to certificate status requests and can issue one of three responses: Valid, Invalid, Unknown. An OCSP responder replies to certificate status requests on the basis of CRLs (Certificate Revocation Lists) provided to it by certification authorities.

**On-line Certificate Status Service (OCSS)** An on-line service, OCSP based, that provides timely information regarding the revocation status of a certificate.

**Private key** The private part of an asymmetric key pair used for public key encryption techniques. The private key is typically used for creating digital signatures or decrypting messages.

**Public key** The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages sent to the owner of the private key.

**Public Key Infrastructure (PKI)** System of CAs (and, optionally, RAs and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.

**Registration Authority (RA)** Optional PKI entity (separate from the CAs) that does not sign either digital certificates or CRLs but has responsibility for recording or verifying some or all of the information (particularly the identities of subjects) needed by a CA to issue certificates and CRLs and to perform other certificate management functions.

**Relying Party** Relying parties use the PKI to implement security services by employing the public key in another user's certificate (exp.: verify digital signature, encrypt data). They may include CAs, RAs, persons, and computing systems such as routers.

**Repository** System for storing and distributing digital certificates and related information (including CRLs, CPSs, and CPs) to certificate users.

**Revocation** To change the status of a valid or suspended certificate to "revoked" from a specified time and forward.

**Root CA** Ultimate CA, which signs the certificates of the subordinate CAs. The root CA has a self-signed certificate that contains its own public key.

**Secret key** A key used in symmetric encryption where the sender and receiver of encrypted messages use the same key for decryption.

**SSL (Secure Sockets Layer)** A popular protocol for managing the security of a message transmission on the Internet. SSL was developed by Netscape and is now also used in products from Microsoft and other Internet client/server developers.

**Subject** A certificate is assigned to a Subject. The Subject can be the holder of the certificate or an organizational role or IT-system for whom the subscriber is responsible and accountable.

**Subscriber** The individual to which the public key certified in a certificate is attributable.

## Acronyms

<b>CA</b>	Certification Authority
<b>CAO</b>	Certification Authority Operator
<b>CASA</b>	Certification Authority Security Administrator
<b>CASO</b>	Certification Authority Security Officer
<b>CMS</b>	Certificate Management System
<b>CN</b>	Common Name
<b>CP</b>	Certificate Policy
<b>CPS</b>	Certification Practice Statement
<b>CRL</b>	Certificate Revocation List
<b>CSS</b>	Certificate Status Service
<b>CU</b>	Certification Unit of NDCA
<b>DN</b>	Distinguished Name
<b>I&amp;A</b>	Identification and Authentication
<b>IETF</b>	Internet Engineering Task Force
<b>FIPS</b>	Federal Information Processing Standards
<b>ITU</b>	International Telecommunications Union
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>NDCA</b>	National Digital Certification Agency
<b>OCSP</b>	On-line Certificate Status Protocol
<b>OCSS</b>	On-line Certificate Status System
<b>OID</b>	Object Identifier
<b>PIN</b>	Personal Identification Number
<b>PKI</b>	Public Key Infrastructure
<b>PKIX</b>	Public Key Infrastructure (X.509) (IETF Working Group)
<b>RA</b>	Registration Authority
<b>RFC</b>	Request for Comments
<b>RSA</b>	A specific Public key algorithm
<b>SSL</b>	Secure Socket Layer
<b>SHA1</b>	Secure Hash Algorithm 1
<b>URL</b>	Uniform Resource Locator
<b>VPN</b>	Virtual Private Network