

---

 National Digital Certification Agency
 

---

# CP / CPS of the Tunisian Server Certificate Authority

## Review

Version	Date	Comment	Page
Version 00	26/06/2015	1st Writing	Whole document
Version 01	28/07/2015	Update	Profiles Update
Version 02	21/10/2015	Update	OCSF Profile Add
Version 03	21/01/2016	Update	Update of the section 9.6.1 Update of sections 1.1, 1.6.1, 1.6.2 and 4.2.1 Adding of section 3.2.5
Version 04	12/02/2016	Update	Update of sections 4.9.9 and 7.1.2
Version 05	18/10/2016	Update	Update of sections 4.9.9 and 5.5.2
Version 06	27/11/2017	Update	Update of section 4.9.9
Version 07	27/02/2018	Update	Update of sections 1.3.2.2, 3.2.2 and 4.2.1

	Author	Validated by	Approved by
<b>Entity :</b>	NDCA	Board Committee	CEO
<b>Date :</b>	26/02/2018	27/02/2018	27/02/2018

## Table of Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>8</b>
1.1	OVERVIEW .....	8
1.2	DOCUMENT NAME AND IDENTIFICATION .....	9
1.3	PKI PARTICIPANTS .....	9
1.3.1	<i>Certification Authority (CA)</i> .....	10
1.3.2	<i>Registration Authorities (RA)</i> .....	11
1.3.2.1	Central Registration Authority (CRA) .....	11
1.3.2.2	Delegated Registration Authority (DRA) .....	11
1.3.3	<i>Publication Service (PS)</i> .....	11
1.3.4	<i>Server Certificate Responsible (SCR)</i> .....	11
1.3.5	<i>Certificate User (CU)</i> .....	12
1.4	CERTIFICATE USAGE .....	12
1.4.1	<i>Appropriate certificate usage</i> .....	12
1.4.1.1	Certificate of the CA .....	12
1.4.1.2	Subscribers' Certificates .....	12
1.4.2	<i>Prohibited Certificate Uses</i> .....	12
1.5	CP/CPS MANAGEMENT .....	12
1.5.1	<i>Organization responsible of this CP/CPS</i> .....	13
1.5.2	<i>Contact person</i> .....	13
1.5.3	<i>Entity determining this CP/CPS implementation conformity</i> .....	13
1.5.4	<i>CP/CPS approval procedures</i> .....	13
1.6	DEFINITIONS AND ACRONYMS .....	13
1.6.1	<i>Acronyms</i> .....	13
1.6.2	<i>Definitions</i> .....	15
<b>2</b>	<b>RESPONSIBILITIES REGARDING THE AVAILABILITY OF INFORMATION TO BE PUBLISHED .....</b>	<b>20</b>
2.1	RESPONSIBLE ENTITIES FOR MAKING INFORMATION AVAILABLE .....	20
2.2	INFORMATION TO BE PUBLISHED .....	20
2.3	TIME AND FREQUENCY OF PUBLICATION .....	20
2.4	ACCESS CONTROLS ON REPOSITORIES .....	21
<b>3</b>	<b>IDENTIFICATION AND AUTHENTICATION .....</b>	<b>22</b>
3.1	NAMING .....	22
3.1.1	<i>Types of names</i> .....	22
3.1.1.1	Certificate of CA Servers .....	22
3.1.1.2	Certificate Bearer .....	22
3.1.2	<i>Need for names to be meaningful</i> .....	23
3.1.3	<i>Pseudonymity of subscribers</i> .....	23
3.1.4	<i>Rules for interpreting various name forms</i> .....	23
3.1.5	<i>Uniqueness of names</i> .....	23
3.1.6	<i>Recognition, authentication, and role of trademarks</i> .....	23
3.2	INITIAL IDENTITY VERIFICATION .....	23
3.2.1	<i>Method to prove possession of private key</i> .....	23
3.2.2	<i>Authentication of Organization and Domain Control</i> .....	23
3.2.3	<i>Validation of the subscriber's identity</i> .....	24
3.2.4	<i>Non-verified subscriber information</i> .....	24
3.2.5	<i>Cross-Certified CA</i> .....	24
3.2.6	<i>Verification of Internationalized Domain Names</i> .....	25
3.3	IDENTIFICATION AND VALIDATION OF RE-KEY REQUESTS .....	25
3.3.1	<i>Identification and validation for routine re-key</i> .....	25
3.3.2	<i>Identification and validation for re-key after revocation</i> .....	25
3.4	IDENTIFICATION AND VALIDATION OF A REVOCATION REQUEST .....	25

<b>4</b>	<b>CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS .....</b>	<b>26</b>
4.1	CERTIFICATE APPLICATION .....	26
4.1.1	Source of a certificate application .....	26
4.1.2	Certificate application Enrollment process and responsibilities .....	26
4.2	CERTIFICATE APPLICATION PROCESSING .....	26
4.2.1	Performing identification and authentication functions .....	26
4.2.2	Approval or Rejection of the Application .....	27
4.2.3	Time to process certificate applications .....	27
4.3	CERTIFICATE ISSUANCE .....	27
4.3.1	CA actions during certificate issuance .....	27
4.3.2	Notification to subscriber by the CA of issuance of certificate .....	28
4.4	CERTIFICATE ACCEPTANCE .....	28
4.4.1	Conduct constituting certificate acceptance .....	28
4.4.2	Publication of the certificate by the CA .....	28
4.4.3	Notification of certificate issuance by the CA to other entities .....	28
4.5	KEY PAIR AND CERTIFICATE USAGE .....	28
4.5.1	Subscriber private key and certificate usage .....	28
4.5.2	Public Key and Certificate Usage by a certificate user .....	29
4.6	CERTIFICATE RENEWAL .....	29
4.6.1	Circumstances for Certificate Renewal .....	29
4.6.2	Source of a Renewal Application .....	29
4.6.3	Procedure for processing a renewal application .....	29
4.6.4	Notification of new certificate issuance to subscriber .....	29
4.6.5	Conduct constituting acceptance of a renewal certificate .....	29
4.6.6	Publication of the new certificate .....	29
4.6.7	Notification of certificate issuance by the CA to other entities .....	30
4.7	CERTIFICATE RE-KEY .....	30
4.8	CERTIFICATE MODIFICATION .....	30
4.9	CERTIFICATE REVOCATION AND SUSPENSION .....	30
4.9.1	Possible causes for revocation .....	30
4.9.1.1	Subscribers' Certificates .....	30
4.9.1.2	Certificates of a component of the PKI .....	31
4.9.2	Who can request revocation .....	31
4.9.2.1	Subscribers' Certificates .....	31
4.9.2.2	Certificates of a PKI Component .....	31
4.9.3	Procedures for revocation request .....	31
4.9.3.1	Revocation of a subscriber's certificate .....	31
4.9.3.2	Revocation of a certificate of a PKI component .....	32
4.9.4	Deadline granted to bearer to make the request of revocation .....	33
4.9.5	Time within which CA must process the revocation request .....	33
4.9.5.1	Revocation of a subscriber's certificate .....	33
4.9.5.2	Revocation of a Certificate of a PKI Component .....	33
4.9.6	Revocation checking requirement for certificate users .....	33
4.9.7	CRL issuance frequency .....	33
4.9.8	Maximum latency for CRLs .....	33
4.9.9	On-line revocation/status checking availability .....	34
4.9.10	Online revocation checking requirements for the certificates users .....	34
4.9.11	Other means of information on revocation available .....	34
4.9.12	Special requirements regarding key compromise .....	34
4.9.13	Possible Circumstances for suspension .....	35
4.9.14	Who can request suspension .....	35
4.9.15	Procedure for processing a suspension request .....	35
4.9.16	Limits on suspension period .....	35
4.10	CERTIFICATE STATUS SERVICES .....	35
4.10.1	Operational characteristics .....	35

4.10.2	<i>Service availability</i> .....	35
4.10.3	<i>Optional features</i> .....	35
4.11	END OF SUBSCRIPTION BETWEEN THE SUBSCRIBER AND THE CA .....	35
4.12	KEY ESCROW AND RECOVERY .....	36
<b>5</b>	<b>NON-TECHNICAL SECURITY MEASURES</b> .....	<b>37</b>
5.1	PHYSICAL SECURITY MEASURES .....	37
5.1.1	<i>Site geographical location and construction</i> .....	37
5.1.2	<i>Physical access</i> .....	37
5.1.3	<i>Power and air conditioning</i> .....	37
5.1.4	<i>Water Exposures</i> .....	37
5.1.5	<i>Fire Prevention and Protection</i> .....	38
5.1.6	<i>Media Storage</i> .....	38
5.1.7	<i>Waste Disposal</i> .....	38
5.1.8	<i>Off-Site Backup</i> .....	38
5.2	PROCEDURAL SECURITY MEASURES .....	38
5.2.1	<i>Trusted Roles</i> .....	38
5.2.2	<i>Number of persons required per task</i> .....	39
5.2.3	<i>Identification and authentication for each role</i> .....	39
5.2.4	<i>Roles requiring separation of duties</i> .....	40
5.3	SECURITY MEASURES REGARDING THE PERSONNEL .....	40
5.3.1	<i>Required qualifications, skills, and empowerment</i> .....	40
5.3.2	<i>Background check procedures</i> .....	40
5.3.3	<i>Initial Training requirements</i> .....	40
5.3.4	<i>Retraining frequency and requirements</i> .....	40
5.3.5	<i>Job rotation frequency and sequence</i> .....	41
5.3.6	<i>Sanctions for unauthorized actions</i> .....	41
5.3.7	<i>Independent Contractor Requirements</i> .....	41
5.3.8	<i>Documentation Supplied to Personnel</i> .....	41
5.4	AUDIT LOGGING PROCEDURES .....	41
5.4.1	<i>Types of Events Recorded</i> .....	41
5.4.2	<i>Frequency of processing log</i> .....	43
5.4.3	<i>Retention Period for Audit Log</i> .....	43
5.4.4	<i>Protection of Audit Log</i> .....	43
5.4.5	<i>Audit Log Backup Procedures</i> .....	43
5.4.6	<i>Event Log Collection System</i> .....	44
5.4.7	<i>Evaluation of vulnerabilities</i> .....	44
5.5	RECORDS ARCHIVAL .....	44
5.5.1	<i>Types of records archived</i> .....	44
5.5.2	<i>Retention period for archive</i> .....	44
5.5.3	<i>Protection of archive</i> .....	44
5.5.4	<i>Archive backup procedure</i> .....	45
5.5.5	<i>Requirements for time-stamping of records</i> .....	45
5.5.6	<i>Archive collection system</i> .....	45
5.5.7	<i>Procedures to obtain and verify archive</i> .....	45
5.6	CHANGING THE CA KEY .....	45
5.6.1	<i>Certificate of CA</i> .....	45
5.6.2	<i>Subscriber's Certificate</i> .....	46
5.7	COMPROMISE AND DISASTER RECOVERY .....	46
5.7.1	<i>Incident and compromise handling procedures</i> .....	46
5.7.2	<i>Recovery procedures in case of corruption of Computing Resources (hardware, software and/or data)</i> 46	
5.7.3	<i>Entity Private Key Compromise Procedures</i> .....	47
5.7.4	<i>Business continuity capabilities after a disaster</i> .....	47
5.8	CA TERMINATION .....	47

5.8.1	<i>Transfer of Activity</i> .....	47
5.8.2	<i>Termination of Activity</i> .....	47
<b>6</b>	<b>TECHNICAL SECURITY CONTROLS .....</b>	<b>49</b>
6.1	KEY PAIR GENERATION AND INSTALLATION .....	49
6.1.1	<i>Key pair generation</i> .....	49
6.1.1.1	CA keys .....	49
6.1.1.2	Keys generated by keys' holders .....	49
6.1.2	<i>Private key delivery to subscriber</i> .....	49
6.1.2.1	CA Private Key .....	49
6.1.2.2	Private keys of the carrier .....	49
6.1.3	<i>Public key delivery to the CA</i> .....	50
6.1.4	<i>CA public key delivery to certificate users</i> .....	50
6.1.5	<i>Key sizes</i> .....	50
6.1.5.1	CA Certificate .....	50
6.1.5.2	Subscriber's certificate .....	50
6.1.6	<i>Public key parameters generation and quality checking</i> .....	50
6.1.7	<i>Key usage purposes</i> .....	51
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS.....	51
6.2.1	<i>Cryptographic module standards and controls</i> .....	51
6.2.1.1	CA Cryptographic Modules .....	51
6.2.1.2	Devices for authentication and signature of bearers.....	51
6.2.2	<i>Private key control by multiple persons</i> .....	51
6.2.3	<i>Private key escrow</i> .....	51
6.2.4	<i>Private key backup</i> .....	51
6.2.4.1	CA private key .....	52
6.2.4.2	Private keys of the bearers .....	52
6.2.5	<i>Private key archival</i> .....	52
6.2.6	<i>Private key transfer into or from a cryptographic module</i> .....	52
6.2.7	<i>CA private key storage on cryptographic module</i> .....	52
6.2.8	<i>Method of activating private key</i> .....	52
6.2.8.1	CA private keys .....	52
6.2.8.2	Private keys of the bearers .....	52
6.2.9	<i>Method of deactivating private key</i> .....	52
6.2.9.1	CA private keys .....	53
6.2.9.2	Private keys of the bearers .....	53
6.2.10	<i>Method of destroying private key</i> .....	53
6.2.10.1	CA private keys .....	53
6.2.10.2	Private keys of the bearers .....	53
6.2.11	<i>Cryptographic Module and devices Rating</i> .....	53
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT .....	53
6.3.1	<i>Public keys archival</i> .....	53
6.3.2	<i>Certificates and key pair lifetimes</i> .....	53
6.4	ACTIVATION DATA .....	54
6.4.1	<i>Activation data generation and installation</i> .....	54
6.4.1.1	Generation and installation of the activation data corresponding to the private key of the CA.....	54
6.4.1.2	Generation and installation of the activation data corresponding to a private key of the bearer .....	54
6.4.2	<i>Activation data protection</i> .....	54
6.4.2.1	Protection of activation data corresponding to the private keys of the CA .....	54
6.4.2.2	Protection of the activation data corresponding to the private keys of the subscribers .....	54
6.4.3	<i>Other aspects of activation data</i> .....	54
6.5	COMPUTER SECURITY CONTROLS .....	55
6.5.1	<i>Specific computer security technical requirements</i> .....	55
6.5.2	<i>Computer systems rating</i> .....	55
6.6	6.6 SYSTEM DEVELOPMENT CONTROLS .....	55
6.7.1	<i>Security Management Measures</i> .....	56
6.7.2	<i>Systems' life cycle security rating</i> .....	56

6.8	NETWORK SECURITY CONTROLS.....	56
6.9	TIME-STAMPING.....	56
<b>7</b>	<b>CERTIFICATES AND CRL PROFILES.....</b>	<b>58</b>
7.1	CERTIFICATE PROFILE .....	58
7.1.1	<i>Certificate of CA</i> .....	58
7.1.2	<i>Subscriber's Certificate</i> .....	59
7.1.3	<i>OCSP Certificate</i> .....	60
7.2	CRL PROFILE.....	61
7.3	OCSP PROFILE .....	62
7.3.1	<i>Version Number</i> .....	62
7.3.2	<i>OCSP Extension</i> .....	62
<b>8</b>	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....</b>	<b>63</b>
8.1	FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT .....	63
8.2	IDENTITY/QUALIFICATIONS OF ASSESSORS.....	63
8.3	RELATIONSHIP BETWEEN THE ASSESSORS AND THE ASSESSED ENTITY .....	63
8.4	TOPICS COVERED BY ASSESSMENT.....	63
8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY .....	64
8.6	COMMUNICATION OF RESULTS .....	64
<b>9</b>	<b>OTHER BUSINESS AND LEGAL MATTERS .....</b>	<b>65</b>
9.1	FEES.....	65
9.1.1	<i>Certificate issuance or renewal fees</i> .....	65
9.1.2	<i>Certificate access fees</i> .....	65
9.1.3	<i>Revocation or status information access fees</i> .....	65
9.1.4	<i>Fees for other services</i> .....	65
9.1.5	<i>Refund Policy</i> .....	65
9.2	FINANCIAL RESPONSIBILITY.....	65
9.2.1	<i>Insurance coverage</i> .....	65
9.2.2	<i>Other assets</i> .....	66
9.2.3	<i>Insurance or warranty coverage for end-entities</i> .....	66
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION .....	66
9.3.1	<i>Scope of confidential information</i> .....	66
9.3.2	<i>Information not within the scope of confidential information</i> .....	66
9.3.3	<i>Responsibilities to protect confidential information</i> .....	66
9.4	PRIVACY OF PERSONAL INFORMATION.....	66
9.4.1	<i>Private information protection policy</i> .....	66
9.4.2	<i>Information treated as private</i> .....	67
9.4.3	<i>Information not deemed private</i> .....	67
9.4.4	<i>Responsibility to protect private information</i> .....	67
9.4.5	<i>Notice and consent to use private information</i> .....	67
9.4.6	<i>Conditions for Disclosure of personal information to judicial or administrative authorities</i> .....	67
9.4.7	<i>Other information disclosure circumstances</i> .....	68
9.5	INTELLECTUAL AND INDUSTRIAL PROPERTY RIGHTS.....	68
9.6	REPRESENTATIONS AND WARRANTIES.....	68
9.6.1	<i>Certification Authorities</i> .....	68
9.6.2	<i>Registration service</i> .....	69
9.6.3	<i>Certificate holders</i> .....	70
9.6.4	<i>Certificate Users</i> .....	70
9.6.5	<i>Other participants</i> .....	70
9.7	DISCLAIMERS OF WARRANTIES .....	70
9.8	LIABILITY.....	70
9.9	INDEMNITIES .....	71
9.10	TERM AND ANTICIPATED TERMINATION OF THIS CP/CPS .....	71

9.10.1	<i>Term</i>	71
9.10.2	<i>Anticipated Termination of validity</i>	71
9.10.3	<i>Effect of termination and remaining applicable provisions</i>	71
9.11	AMENDMENTS TO THE CP/CPS	71
9.11.1	<i>Procedures for amendments</i>	71
9.11.2	<i>Mechanism and reporting period for amendments</i>	72
9.11.3	<i>Circumstances under which an OID is to be changed</i>	72
9.12	CONFLICT RESOLUTION PROVISIONS	72
9.13	COMPETENT JURISDICTIONS	72
9.14	COMPLIANCE WITH LAWS AND REGULATIONS	72
9.15	MISCELLANEOUS PROVISIONS	72
9.15.1	<i>Global agreement</i>	73
9.15.2	<i>Transfer of business</i>	73
9.15.3	<i>Consequences of an Invalid Clause</i>	73
9.15.4	<i>Application and Waiver</i>	73
9.15.5	<i>Force majeure</i>	73
9.16	MISCELLANEOUS PROVISIONS	73
<b>10</b>	<b>REFERENCES</b>	<b>74</b>



# 1 INTRODUCTION

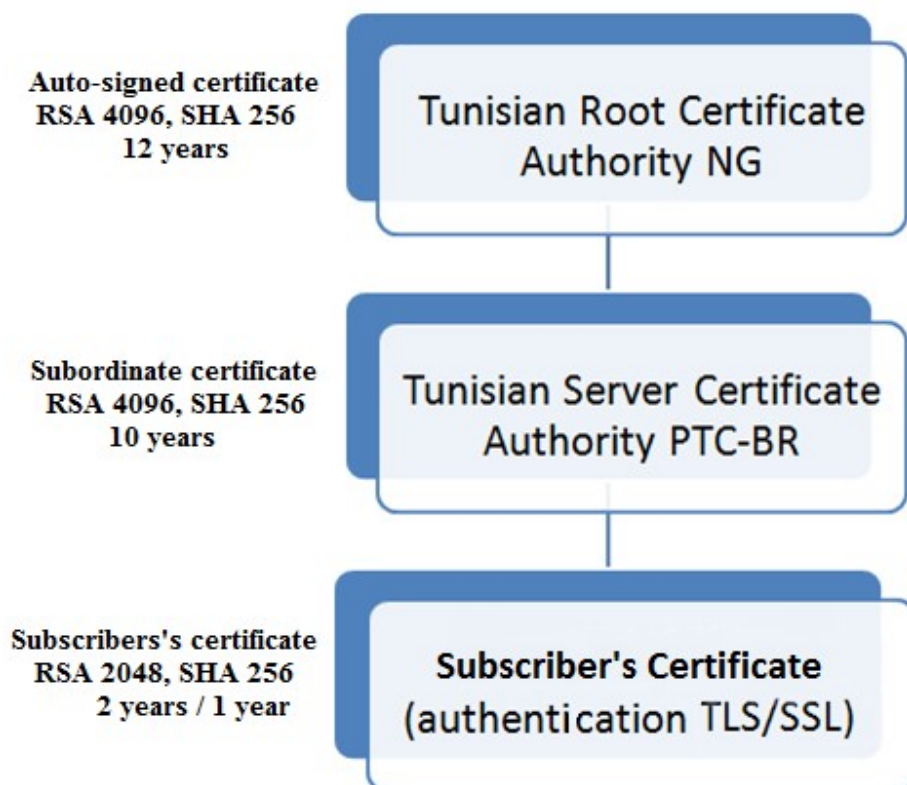
---

## 1.1 Overview

The NDCA, the National Agency for Electronic Certification, is the repository of electronic trust in Tunisia. The NDCA is in charge in particular of the creation and operation of the National Root Certification Authority of Tunisia.

In this perspective, the NDCA implements its PKI, structured as a Root Authority and subordinate authorities, specialized by targeted populations or uses (physical persons, servers, VPN equipments, code signing, etc.).

The hierarchy of the NDCA's PKI subject of this document is structured as follows:





 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 9/74  NC: PU</p>
---	---	---

The "Tunisian Server Certificate Authority PTC BR", or "the CA Servers" in the rest of the document, is responsible for issuing the electronic certificates of authentication of the SSL servers.

The CA servers complies with the current version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (BR) published at <http://www.cabforum.org>. In the event of inconsistency between this document and the CAB Forum BR requirements, the CAB Forum BR requirements apply.

The CA servers is certified by the NDCA's trusted anchor, entitled "Tunisian Root Certificate Authority NG", known as "Root CA NG" under the responsibility of the NDCA.

The purpose of this document is to describe the requirements applicable on certification practices that are to be implemented by the CA for the issuance of certificates for the use of TLS / SSL server authentication.

This document is prepared in a manner that is generally consistent with the plan of the IETF RFC 3647 "X.509 Public Key Infrastructure Certificate Policy Certification Practice Statement Framework". On the other hand, no compliance requirement is established with respect to this RFC directly in this document. The retained compliance is with ETSI TS 102 042 PTC-BR for the CP / CPS of the CA.

In the rest of the document, the generic term "CA" can be used to replace "CA Servers (of the NDCA)".

## 1.2 Document Name and identification

This CP/ CPS document entitled "Certification Policy and Certification Practices Statement of the Tunisian Server Certificate Authority PTC BR" is owned by NDCA.

It is identified by the following unique identifier OID : 2.16.788.1.2.6.1.8.

## 1.3 PKI Participants

The CA uses the following components and sub-components:

- **Registration service:** this service is also called "Registration Authority" (RA). There are two types of RA entities:
  - the Central Registration Authority ("CRA"), provided by the NDCA to manage requests for certificates and revocation,
  - Delegated Registration Authorities "DRA" at the level of the partners' counters to collect requests for certificates and transfer them to the CRA, which is responsible for checking their consistency and validating their content;

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 10/74 NC: PU
---	--	---

- **Production of certificates, CRLs:** this service is provided by the NDCA, which generates the electronic certificates of the bearers from the information transmitted by the registration service after having previously verified and validated them. Finally, this service communicates to the CRA the certificates produced for delivery to the SCR;
- **Bearer delivery service:** this service delivers to the SCR the authentication server certificate;
- **Publishing service:** this service makes available to users of certificates (CU) through a website the information necessary for the use of the certificates issued by the CA (general conditions, CP / CPS published by the CA, certificates of CA, ...), as well as the validity information of the certificates resulting from the processing of the revocation management service (CRL, information notice, ...);
- **Revocation management service:** This service processes revocation requests for server certificates received online or at the CRA level. The processing results are disseminated through the certificate status information service;
- **Certificate Status Information Service:** This service provides certificate users (CU) with information about the status of certificates. This function is implemented according to a method of publishing information updated at regular intervals in the form of Certificate Revocation Lists (CRL).
- **Logging service:** this service is implemented by all the technical components of the PKI. It is provided by the NDCA. It allows to collect all the data used and / or generated in the context of the implementation of the services of the PKI in order to obtain traces of audits that can be consulted.
- **audit service:** this service is provided by the internal auditing entity at the NDCA, which is responsible for the application of regular and recurring controls to ensure conformity of practices with the CP / CPS.

### 1.3.1 Certification Authority (CA)

The NDCA acts as a CA and ensures the consistency and management of the safety repository, as well as its implementation. The CA security repository is composed of the Information Systems Security Policy and this CP / CPS, the General Terms and Conditions of Use (GTCU) and all the procedures implemented by the components of the PKI.

The NDCA validates the security repository and authorizes and validates the creation and use of the CA components. It follows the audits and / or conformity controls carried out on the components of the PKI, decides on the actions to be carried out and ensures that they are implemented.

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 11/74 NC: PU
---	--	---

The CA is responsible for ensuring the link between the identifier of a server and the associated SCR and cryptographic keys for a given use. This warranty is provided by public key certificates that are signed by a private key of the CA.

The CA generates certificates and revokes certificates based on requests sent from the Registration Authority. In addition to Certificate Lifecycle Management Services, the CA implements logging and auditing services.

The CP / CPS, public keys and CRLs issued by the CA are the property of the CA.

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

The registration authority (RA) consists of:

- the Central Registration Authority "CRA";
- the Delegated Registration Authorities "DRA" at partner's counters.

#### **1.3.2.1 Central Registration Authority (CRA)**

The NDCA provides the role of CRA, which is responsible for:

- registration for certificate requests;
- revocation of certificates;
- the issuing of server certificates to the SCR that went to the NDCA's counter.

#### **1.3.2.2 Delegated Registration Authority (DRA)**

The partners who have signed an agreement with the NDCA, ensure the role of DRA.

The DRAs are responsible for the collection of certificate requests and their transmission to the CRA. The domain validation is only performed by the CRA of TunServerCA2 as described in section 3.2.2.

### **1.3.3 Publication Service (PS)**

The SP is used to implement the publication of documents such as CP / CPS (more details are provided in section 2).

### **1.3.4 Server Certificate Responsible (SCR)**

In the context of this CP / CPS, a Server Certificate Responsible (SCR) is a natural person who is responsible for using the certificate of the server or computer device identified in the certificate and the private key corresponding to this certificate, on behalf of the entity identified in that certificate. The SCR is contractually, hierarchically or legally bound to this entity.

The SCR must comply with the requirements set out in this CP / CPS.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 12/74  NC: PU</p>
---	---	--

Because the certificate is attached to the server (or to the device) and not to the SCR, the latter may change during the term of the certificate. In this case, the entity must first inform the CA of the departure of the SCR from its functions and designate a successor. Otherwise, where there is no explicitly identified SCR for a given certificate, it must be revoked.

### 1.3.5 Certificate User (CU)

The CU is an application, a physical or legal entity, an administrative body or a hardware computer system that uses a server certificate in accordance with the requirements of this CP / CPS.

In this CP / CPS, a CU, to ensure the validity of a bearer's certificate, must construct and validate a certification path from the bearer's certificate to a auto-signed trusted anchor - which in the circumstances may be that of the NDCA. The CU must also control the revocation information for each element of the certification path (CRL for the server certificate and ARL for CA certificates).

## 1.4 Certificate Usage

### 1.4.1 Appropriate certificate usage

#### 1.4.1.1 Certificate of the CA

The CA key is used to sign bearer's certificates and Certificate Revocation Lists (CRLs)

#### 1.4.1.2 Subscribers' Certificates

This CP / CPS allows to issue certificates for the SCR defined in the section above, for the use of authentication in the context of a secure TLS / SSL session.

The Certificate User (CU) uses the server certificate to validate the identity of the server's domain name and establish the session key for encrypted data exchange.

### 1.4.2 Prohibited Certificate Uses

Any use not specified in this CP / CPS is prohibited.

Thus, the NDCA may not be held liable for the use of certificates issued under this CP / CPS for purposes and on terms other than those provided for in this CP / CPS.

## 1.5 CP/CPS Management

 <small>Agence Nationale de Certification Electronique</small>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 13/74 NC: PU
--	--	---

### 1.5.1 Organization responsible of this CP/CPS

The NDCA is responsible of the establishment, control and updating, when necessary, of the current CP/CPS.

### 1.5.2 Contact person

The remarks concerning this CP / CPS should be sent to

Name of the Responsible Entity	Email Address	Mail Address
National Digital Certification Agency	ance@certification.tn	Technopark El Ghazala. Road of Raoued, Km 3.5 2083 Ariana, - Tunisia

### 1.5.3 Entity determining this CP/CPS implementation conformity

The NDCA carries out conformity analyzes/controls and/or audits which lead to the authorization or not for the CA to issue certificates.

### 1.5.4 CP/CPS approval procedures

The NDCA has its own methods of approving this document. The NDCA approves the results of the compliance review by the experts appointed for this purpose in accordance with the procedure for updating the CP / CPS.

## 1.6 Definitions and Acronyms

### 1.6.1 Acronyms

ARL	Authority Revocation List
ARLDP	Authority Revocation List Distribution Point
CA	Certification Authority
CAA	Certification Authority Authorization

CN	Common Name
CP	Certification Policy
CPS	Certification Practice Statement
CRA	Central Registration Authority
CRL	Certificate Revocation List
CRLDP	Certificate Revocation List Distribution Point
CSR	Certificate Signing Request
CU	Certificate User
DN	Distinguished Name
DRA	Delegated Registration Authority
ETSI	European Telecommunications Standards Institute
GCU	General Conditions of Use
HTTPS	HyperText Transfer Protocol Secure
IDN	Internationalized Domain Name
ISO	International Organization for Standardization
ISSP	Information Systems Security Policy
LDAP	Lightweight Directory Access Protocol
NDCA	National Digital Certification Agency

NTP	Network Time Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PS	Publication Service
RA	Registration Authority
RFC	Requests For Comments
RSA	Rivest Shamir Adleman
SCR	Server Certificate Responsible
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

### 1.6.2 Definitions

**Audit:** independent control of records and activities of a system to assess the adequacy and effectiveness of system controls, verify compliance with established operational policies and procedures, and recommend necessary changes in controls, policies , or procedures.

**Certification Authority (CA):** entity responsible for guaranteeing the link (unfalsifiable and univocal) between the identifier of a bearer and a cryptographic key pair for a given use. This warranty is provided by public key certificates that are signed by a private key of the CA.



 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 16/74 NC: PU
---	--	---

**Registration Authority (RA)** : entity responsible for issuing certificates to the SCR. The RA also deals with certificate requests. The RA is a generic term used to refer to the CRA at the NDCA's counter or a DRA at the partner's counters.

**Central Registration Authority (CRA)**: The central registration authority is provided by the NDCA. It is responsible for the registration services and the issuing of certificates to the SCR.

**Delegated Registration Authority (DRA)**: the delegated registration authority is ensured at the level of the partners' counters. ~~It is responsible for the registration services and the issuing of certificates to the SCR.~~

**Common Criteria**: A set of security requirements that are described according to an internationally recognized formalism. Products and software are evaluated by a laboratory to ensure that they have mechanisms to implement the selected security requirements for the product or software being evaluated.

**Key ceremony**: A procedure whereby a CA key pair is generated, its private key transferred and most likely backed up, and / or its public key is certified.

**Electronic certificate**: An electronic file attesting that a public key is linked to the domain name identified in the certificate. It is issued by a Certification Authority. By signing the certificate with its private key, the CA validates the link between the identifier of the domain name and the key pair and guarantees its authenticity.

**Certificate of CA**: certificate for a CA issued by another CA. [X.509].

**Certificate of self-signed CA**: CA certificate signed by the private key of this same CA.

**Challenge**: a list of alphanumeric characters used as a secret and communicated to the certificate bearer during registration in order to allow simplified management of bearer information and their certificates.

**Certification path**: (or chain of trust, or chain of certification) chain consisting of several certificates required to validate a certificate against a self-signed CA certificate.

**Private key**: key of the asymmetric key pair of an entity to be used only by that entity [ISO / IEC 9798-1].

**Public key**: key of the asymmetric key pair of an entity that can be made public [ISO / IEC 9798-1].

**Customer**: Organization, legal or natural person, professional who contracts with the NDCA to have certificates.

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 17/74 NC: PU
---	--	---

**Component:** platform operated by an entity and consisting of at least one computer station, an application and, where appropriate, a cryptology means and playing a determined role in the operational implementation of at least one function of the PKI.

**Compromise:** breach, proven or suspected, of a security policy, during which unauthorized disclosure, or loss of control of sensitive information, may have occurred. In the case of private keys, a compromise is constituted by the loss, theft, disclosure, modification, unauthorized use or other compromises of this private key.

**Confidentiality:** The ownership of information not to be made available or disclosed to unauthorized individuals, entities, or processes.

**Contract:** a contractual set made up of the general conditions of use, the certificate application form and the procedures on the website [www.certification.tn](http://www.certification.tn) applicable on the date of conclusion of the contract.

**Certification Practice Statement (CPS):** A document that identifies and refers to the practices (organization, operational procedures, technical and human resources) that CA applies in the context of the provision of its electronic certification services to users and in accordance with the certification policy (s) it has undertaken to comply with.

**Certificate Request:** A message sent by a RA entity to the CA to obtain the issuance of a CA certificate.

**Availability:** feature of being available on request, to an authorized entity [ISO / IEC 13335-1: 2004].

**Activation data:** data values, other than keys, which are required to operate the cryptographic modules or the elements they protect and which must be protected (for example a PIN, a passphrase, etc.).

**Hash function:** a function that binds bit strings to bit strings of fixed length, thus satisfying the following three features:

- It is impossible, by a calculation means, to find, for a given output, an input corresponding to this output;
- It is impossible, by a calculation means, to find, for a given input, a second input corresponding to the same output [ISO / IEC 10118-1];
- It is impossible by calculation to find two different input data that correspond to the same output.

**Key Management Infrastructure (KMI):** A set of components, functions, and procedures for managing cryptographic keys used by trusted services.

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 18/74 NC: PU
---	--	---

**Public Key Infrastructure (PKI):** KMI dedicated to the management of asymmetric keys. This is the infrastructure required to produce, distribute, manage public and private keys, certificates, and Certificate Revocation Lists.

**Integrity:** refers to the accuracy of the information, the source of the information, and the operation of the system that processes it.

**Interoperability:** implies that the equipment and procedures used by two or more entities are compatible; and as a consequence it is possible for them to undertake joint or combined activities.

**Certificate Revocation List (CRL):** A list that is digitally signed by a CA and that contains certificate identities that are no longer valid. The list contains the identity of the CA CRL, the date of publication, the date of publication of the next CRL and the serial numbers of the revoked certificates.

**Representative Agent:** A person, directly or indirectly, that has by law, by delegation or by power of attorney of the client, the power to perform any act necessary for the request of issuing and the conclusion and execution of the contract in addition to the obligations relating to the management of any certificate bearing the name of the client, which shall have been issued at the request and under the responsibility of the said natural or legal person in the absence of an express designation, the representative is a legal representative of the client. The representative agent is responsible for the actions of the holders.

**Cryptographic module:** A set of software and hardware components used to implement a private key in order to enable cryptographic operations (signature, encryption, authentication, key generation ...). In the case of a CA, the cryptographic module is an evaluated and certified hardware cryptographic resource (FIPS or common criteria) used to maintain and implement the CA private key.

**Domain name:** It is composed of the name preceding the extension and completed by the extension itself. The domain name must always be registered in the name of the organization requesting it. During the registration process, the domain name is "associated" with a technical contact which is legally authorized to use that domain name.

**Internationalized Domain Name:** is a domain name that contains (potentially) non-ASCII characters.

**Certificate validity period:** The period during which the CA warrants that it will maintain information about the validity of the certificate. [RFC 2459].

**PKCS # 10:** (Public Key Cryptography Standard #10) developed by RSA Security Inc., which defines a structure for a Certificate Signing Request (CSR).

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 19/74  NC: PU</p>
---	---	--

**Disaster recovery plan** : means a plan defined by a CA to reinstate all or part of its PKI services after they have been damaged or destroyed as a result of a disaster, while not exceeding a deadline set in the CP / CPS.

**CRL distribution point**: directory entry or other CRL broadcasting source; a broadcasted CRL through a CRL distribution point may include revocation entries for only a subset of the set of certificates issued by a CA, or may contain revocation entries for multiple CAs. [ISO / IEC 9594-8; ITU-T X.509].

**Certification Policy (CP)**: a set of rules, identified by a name (OID), defining (a) the requirements that a CA complies with in setting up and providing its services and indicating the applicability of a certificate to a particular community and / or class of applications with common security requirements; and (b) obligations and requirements for other stakeholders, including certificate holders and users.

**CP and CPS**: merging the Certification Policy (CP) and Certification Practice Statement (CPS)

**Security policy**: A set of rules issued by a security authority relating to the use, provision of security services and facilities [ISO / IEC 9594-8; ITU-T X.509].

**Secret Holder**: A person who holds an activation data related to the implementation of the private key of a CA using a cryptographic module.

**Policy Qualifier**: Policy information that goes with a Certificate Policy ID (OID) in a X.509 certificate. [RFC 3647]

**RSA**: public key cryptography algorithm invented by Rivest, Shamir, and Adleman.

**Digital signature**: A cryptographic checksum generated using a hash function and a private key and verifiable by using a public key.

**User of Certificates (UC)**: An application, a natural or legal person, administrative body or hardware computer system that uses a carrier's certificate in accordance with this CP / CPS in the context of an electronic signature.

**Validation of an electronic certificate**: a checking operation that ensures that the information contained in the certificate has been verified by one or more certification authorities (CA) and is still valid. The validation of a certificate includes verification of its validity period, its status (revoked or not), the identity of the CAs and the verification of the electronic signature of all CAs contained in the certification path. It also includes certificate validation for all CAs in the certification path. The validation of an electronic certificate requires first to choose the self-signed certificate that will be taken as a reference.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 20/74  NC: PU</p>
---	---	--

## 2 Responsibilities regarding the availability of information to be published

### 2.1 Responsible Entities for making information available

The Publishing Service (PS) is the service responsible for the publication of this document and other documents or information whose publication is necessary to ensure the proper use of the certificates issued under this CP / CPS.

The PS is responsible for making available the information listed below on the NDCA's website.

### 2.2 Information to be published

The CA ensures that the terms and conditions applicable to the use of the certificates it issues are made available to holders and CUs.

The CA, through the PS, makes available the following information:

- This CP / CPS (<http://www.certification.tn/sites/default/files/documents/CPCPS-PTC-BR-EN-07.pdf>);
- The General Conditions of Use (GCU) of the certificates (<http://www.certification.tn/rpa>);
- The certificate application form (<http://www.certification.tn/en/content/forms-of-certificates-electronic>);
- The certificate revocation application form (<http://www.certification.tn/fr/content/formulaires-de-certificats-electroniques>);
- The CA certificate (<http://www.certification.tn/pub/TunServerCA2.crt>);
- Certificates of the chain of trust to which the CA is attached, including the NDCA CA Root Certificate (<http://www.certification.tn/pub/TunRootCA2.crt>);
- Valid and Updated Certificate Revocation List (CRL) (<http://www.certification.tn/pub/TunServerCA2.crl>) and  
URL=[ldap://ldap.certification.tn/cn=Tunisian Server Certificate Authority PTC BR - TunServerCA2,dc=certification,dc=tn?certificateRevocationList;binary?base?objectclass=crlDistributionPoint](ldap://ldap.certification.tn/cn=Tunisian%20Server%20Certificate%20Authority%20PTC%20BR%20-%20TunServerCA2,dc=certification,dc=tn?certificateRevocationList;binary?base?objectclass=crlDistributionPoint)

All this information is available on the NDCA's website, available at [www.certification.tn](http://www.certification.tn).

### 2.3 Time and Frequency of Publication

 Agence Nationale de Certification Electronique	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 21/74 NC: PU
---	--	---

This CP / CPS and the CA Servers certificates and the NDCA Root CA are permanently available at a 24/7 availability rate and updated as required.

A new CRL is published every 24 hours following a 24/7 availability rate.

## **2.4 Access controls on repositories**

The information published on the website, detailed in § 2.2, are publicly accessible as read-only. The writing privilege to the published information is strictly limited to the authorized persons of the NDCA. Administrators authenticate using strong authentication. Communication between administrators and servers is encrypted to ensure confidentiality.

 <small>Agence Nationale de Certification Electronique</small>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 22/74 NC: PU
--	--	---

## 3 Identification and Authentication

### 3.1 Naming

#### 3.1.1 Types of names

In each X.509 certificate, the CA (Issuer) and the bearer (Subject) are identified by a Distinguished Name (DN). The identifiers used in these certificates conform to X.500.

##### 3.1.1.1 Certificate of CA Servers

The identifiers used in the CA Server Certificate are as follows:

Basic field	Value
Issuer DN	C=TN O=National Digital Certification Agency CN=Tunisian Root Certificate Authority - TunRootCA2
Subject DN	C=TN O=National Digital Certification Agency CN=Tunisian Server Certificate Authority – TunServerCA2

##### 3.1.1.2 Certificate Bearer

The identity of the holder in the holder's certificate is as follows:

Basic field	Value
Issuer DN	C=TN O=National Digital Certification Agency CN=Tunisian Server Certificate Authority – TunServerCA2
Subject DN	C = (Required) ISO country code of the competent authority with which the NDCA's client organization is officially registered. This code is written in uppercase; O = (Required) Full official name of the client organization as it is registered with the competent authorities (Ministry of Commerce, ...) or the abbreviation of the organization. OU = (Optional) Department of the SCR CN = (Required) Domain Name. This entry must be in the subject



 <small>Agence Nationale de Certification Electronique</small>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 23/74 NC: PU
--	--	---

	Alternative Name. Email = (Required) Email Address of the SCR L = (Required) City of client organization
--	--

### 3.1.2 Need for names to be meaningful

The server names included in the certificates issued in accordance with this CP / CPS are always explicit and nominative.

### 3.1.3 Pseudonymity of subscribers

This CP / CPS does not allow pseudonyms and anonymous names in issued certificates.

### 3.1.4 Rules for interpreting various name forms

The identification of the server or device is based on its FQDN (Fully Qualified Domain Name).

### 3.1.5 Uniqueness of names

DNs of server certificates are unique within the certification domain of the CA issuing the certificate. During the lifetime of the CA Servers, a DN assigned to a client cannot be assigned to another client.

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

Not applicable for trademarks.

## 3.2 Initial Identity Verification

### 3.2.1 Method to prove possession of private key

Proof of ownership of the private key by the server is carried out by the procedures for generating the private key corresponding to the public key to be certified and through the means of transmission of the public key (see § 6.1).

### 3.2.2 Authentication of Organization and Domain Control

The RA of the TunServerCA2 validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures listed in section 3.2.2.4 of

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 24/74  NC: PU</p>
---	---	--

the Baseline Requirements. More specifically, the following methods are regularly utilized to fulfill the requirements for authenticating Domain Control:

- Phone call to the Domain Contact’s phone number, as provided by the Domain Registrar, and receiving confirmation that the Applicant has requested validation of the Domain Name, performed in accordance with BR Section 3.2.2.4.3;
- Constructed Email to Domain Contact establishing the Applicant’s control over the FQDN by sending an e-mail created by using ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’ or ‘postmaster’ as the local part followed by the (“@”) sign, followed by an Authorization Domain name, including a Random Value in the e-mail, and receiving a response using the Random Value, performed in accordance with BR Section 3.2.2.4.4;
- An Agreed-Upon Change to the Website by the Applicant placing an agreed-upon Request Token or Request Value in the “/.well-known/pki-validation” directory, performed in accordance with BR Section 3.2.2.4.6.

### **3.2.3 Validation of the subscriber's identity**

Authentication of a client organization is done by checking the following documents:

- The certificate application form duly completed and signed by the applicant, acting as a certificate request, containing in particular the postal address, the professional e-mail address and the telephone number enabling the NDCA to contact the future bearer;
- A copy of the National Identity Card, passport or residence card of the applicant and the SCR;
- An extract from the trade register not exceeding three months;

The bearer must be informed that the personal identity information he has provided for the registration file will be retained.

The verification and validation of the request are carried out in accordance with the provisions described in section § 4.2.

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

This CP / CPS does not make any requirement on this point.

### **3.2.5 Cross-Certified CA**

This CP / CPS does not forecast for cross-certification of CA Servers with other CAs.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 25/74  NC: PU</p>
---	---	--

### 3.2.6 Verification of Internationalized Domain Names

The CA Servers does not allow internationalized domain names in the certificates it generates.

## 3.3 Identification and validation of re-key requests

The renewal of the key pair of a subscriber involves the generation and provision of a new certificate. The procedure is identical to the certificate generation procedure. In all cases, the registration information are checked once more. In case of change detection, the necessary supporting documents must be provided. In addition, a new certificate cannot be provided to the bearer without renewal of the corresponding key pair (see § 4.6).

### 3.3.1 Identification and validation for routine re-key

The renewal of the certificate is similar to a renewal of the key pair and the assignment of a new certificate in accordance with the initial procedures described in section § 4.2.

### 3.3.2 Identification and validation for re-key after revocation

The renewal of a certificate is similar to a renewal of the key pair and the assignment of a new certificate in accordance with the initial procedures described in § 4.9.

## 3.4 Identification and validation of a revocation request

The revocation request may be made:

- Through the physical presence of the SCR or the person in charge at the RA's counter by means of a duly signed revocation application form. The identity of the SCR or the person in charge must be verified by the revocation management service.

The form contains information communicated under cover called the challenge. It must be disclosed in the revocation application.

- Through the NDCA's website through the personal space (<https://eservices.certification.tn>), following the authentication of the applicant based on the challenge,
- Through an internal revocation request by one of the components of the PKI in accordance with the provisions described in section § 4.9.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 26/74  NC: PU</p>
---	---	--

## 4 Certificate Life-Cycle Operational Requirements

### 4.1 Certificate application

#### 4.1.1 Source of a certificate application

A certificate can be requested by a legal representative of the organization to which the server is implemented.

#### 4.1.2 Certificate application Enrollment process and responsibilities

The following information shall at least form part of the certificate application:

- The FQDN of the server to be used in the certificate;
- The name and surname of the SCR;
- The personal identification data of the SCR as well as the legal representative including a valid official document of identity, including a photograph of identity;
- Information enabling the RA to contact the SCR (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", " hostmaster ", or" postmaster "@ the name of the requested domain;
- The General Conditions of Use (GCU) signed by the legal representative;
- An official extract from the trade register of the organization dating no longer than three months;
- A certificate of non-bankruptcy for private organizations.
- The CSR for the public key to be signed.
- A power of attorney for applications for certificates filed by an agent.

The application file is drawn up and signed by the legal representative of the organization.

### 4.2 Certificate application processing

#### 4.2.1 Performing identification and authentication functions

For the purpose of verifying the identities of the applicants, the RA performs the following operations:

- check the consistency of the registration file and the supporting documents submitted;

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 27/74  NC: PU</p>
---	---	--

- verify the accuracy of the purchase order and payment;
- verify that the organization holds the domain name according to the procedure described in section 3.2.2.
- ensure that the SCR is aware of the terms and conditions applicable to the use of the certificate.
- checks the DNS for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, according to the procedure in RFC 6844. The CRA of the TunServerCA2 checks for relevant CAA records prior to issuing certificates. The CRA acts in accordance with CAA records if present. The Certification Authority CAA identifying domains for CAs within TunServerCA2's operational control are "ance.tn", "certification.tn", "tuntrust.tn".

Upon completion of these operations, the RA sends the request to the CA components responsible for certificate production. The RA then retains a copy of the proof of identity submitted in paper or electronic form having a legal value.

#### **4.2.2 Approval or Rejection of the Application**

Upon acceptance of the application, the RA sends the request to the CA.

If the application is rejected, the RA shall inform the applicant (s) by specifying the reason for the rejection and the list of incorrect or incomplete fields.

The rejection decision is taken at the time of filing of the application file or at the validation stage for online applications.

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

The application for a certificate is processed on receipt of the application and settlement of the payment by the RA as soon as possible.

### **4.3 Certificate issuance**

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

The RA sends the certification request to the CA.

The CA generates the SSL server certificate.

The CA sends the certificate to the RA.

The certificate is delivered to the SCR either by sending it by post or by hand delivery or by the CRA at the NDCA's counter or by a DRA at one of the partners' counters.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 28/74  NC: PU</p>
---	---	--

The communications between the various components of the PKI cited above are authenticated and protected in integrity and confidentiality.

The conditions for the generation of certificates and the safety measures are specified in sections 5 and 6 below.

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

The certificate is delivered to the SCR by the RA by e-mail or at the CRA's counter or at one of the DRA's.

## **4.4 Certificate acceptance**

### **4.4.1 Conduct constituting certificate acceptance**

As soon as the certificate is received by the SCR, the CA Server considers the certificate as accepted. Acceptance is tacit. In the event of a dispute within seven (07) working days, the SCR alerts the RA and requests the revocation of his certificate.

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

The CA certificate and server certificates issued by CA Servers are published by the PS.

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

The applicant is informed of the issuance of an SSL certificate for the domain name (s) for which he is responsible. The CRA department is also informed of the issuance of the certificate.

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

### **4.5.1 Subscriber private key and certificate usage**

In accordance with section § 1.4, the use of the private key and the certificate issued by the CA Servers is strictly limited for purposes of authentication and TLS / SSL session establishment, in accordance with this CP / CPS . The SCR must respect the authorized use of key pairs and certificates. Their liability may be incurred in the opposite case.

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 29/74 NC: PU
---	--	---

In addition, authorized uses must be included in the certificate itself, through the key usage extensions ("Key Usage" and "Extended Key Usage" fields of X509 v3 in accordance with section § 7.1).

#### **4.5.2 Public Key and Certificate Usage by a certificate user**

In accordance with section § 1.4, users of certificates are required to strictly respect the authorized uses of certificates issued under this CP / CPS. Otherwise, their liability could be incurred.

### **4.6 Certificate renewal**

The certificate renewal process is similar to the certificate generation process (see previous sections). The certificate renewal operation is independent from the expired certificate. The renewal service is supplemented by automatic notification of clients of the expiration of their certificate two (2) times by email, in the last two weeks before expiration.

#### **4.6.1 Circumstances for Certificate Renewal**

A key pair and a certificate may be renewed because the certificate is about to expire or following revocation of the holder's certificate (see § 4.9).

#### **4.6.2 Source of a Renewal Application**

Same as described in section § 4.1.1.

#### **4.6.3 Procedure for processing a renewal application**

Same as described in section § 4.2.

#### **4.6.4 Notification of new certificate issuance to subscriber**

Same as described in section § 4.3.

#### **4.6.5 Conduct constituting acceptance of a renewal certificate**

Same as described in Section 4.4.1.

#### **4.6.6 Publication of the new certificate**

Same as described in Section 4.4.2.



 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 30/74  NC: PU</p>
---	---	--

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

Same as described in Section 4.4.3.

### **4.7 Certificate Re-Key**

This section concerns the generation of a new certificate with the change of the associated public key. Changing the public key of a certificate implies creating a new certificate. In this case, the procedure for renewing an SSL certificate is identical to that described for issuing the first certificate (see section § 4.1 above).

### **4.8 Certificate modification**

Certificate modification is not permitted in this CP / CPS.

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

#### **4.9.1 Possible causes for revocation**

##### **4.9.1.1 Subscribers' Certificates**

The following circumstances may result in revocation of a subscriber's certificate:

- The inconsistency of the server information on the certificate with the intended use of this certificate before the normal expiry of the certificate;
- the SCR has not complied with the applicable terms and conditions of use of the certificate;
- the carrier's private key is suspected of compromise, is compromised, is lost or is stolen;
- The SCR or an authorized entity (legal representative of the entity) requests revocation of the certificate (in particular in the case of destruction or alteration of the private key associated with the certificate);
- The cessation of activity of the organization;
- An error (intentional or not) has been detected in the record or in the registration process;
- Changes in cryptographic characteristics imposed by relevant national or international institutions;
- The revocation of the CA;

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 31/74  NC: PU</p>
---	---	--

- The end of life of the CA.

When one of the above circumstances is realized and the CA is aware of it (it is informed of it or it obtains the information during one of its audits, when issuing a new certificate, for example) , the concerned certificate must be revoked.

#### **4.9.1.2 Certificates of a component of the PKI**

The following circumstances may result in the revocation of a certificate of a PKI component (including a CA Certificate for Certificate issuance, of CRL):

- the component's private key is suspected of being compromised, compromised, lost or stolen;
- decision to change the PKI component following the detection of a non-conformity of the procedures applied within the component with those announced in the CP / CPS (for example, following a negative qualification or conformity audit) ;
- Termination of activity of the entity operating the component.

### **4.9.2 Who can request revocation**

#### **4.9.2.1 Subscribers' Certificates**

The SCR or the legal representative may request revocation of a certificate issued under this CP / CPS. The CA Servers issuing the certificate or one of its components may request revocation of certificates issued under this CP / CPS.

#### **4.9.2.2 Certificates of a PKI Component**


The revocation of a CA certificate can only be decided by the entity responsible for the CA, or by the judicial authorities via a court decision.

The revocation of the other components' certificates is decided by the CA itself.

### **4.9.3 Procedures for revocation request**

#### **4.9.3.1 Revocation of a subscriber's certificate**

The requirements for identifying and validating a revocation request are described in Section 3.4. The filing of the revocation request is available via three channels:

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 32/74  NC: PU</p>
---	---	--

- The NDCA's counter: a paper form is made available to clients at the NDCA's counter for the revocation of certificates. It is also possible to download and print the same form available on the website to send it by mail or fax to the NDCA. The revocation application form must be completed and signed by the applicant.
- Partners' counters: The same paper form is available to clients at the counters of partners for revocation of certificates. The revocation application form must be duly completed and signed by the applicant.
- Website: the SCR or the legal representative can make the revocation from his personal space on the NDCA's website.

The following information must be included at least, in a certificate revocation request:

- the identity of the certificate server used in the certificate: FQDN;
- the file number enabling the certificate to be retrieved quickly for revocation;
- the cause of revocation;
- the challenge communicated in advance in the envelope under cover. This information is not mandatory in the case of the physical presence of the applicant at the RA's counters.

The RA authenticates the revocation request and carries out the appropriate checks.

The DRAs forward the requests to the CRA. This authenticates the DRA and carries out the appropriate checks.

The CRA forwards the request to the CA responsible for the production of certificates and CRLs. The CA then performs the revocation and generation of the CRL.

The PS then carries out the publication of the CRL containing the revocation information and updates the OCSP server.

The causes of revocation are not published either in the CRL or on the OCSP server.

The applicant for revocation is informed that his application has been taken into account and that the certificate has been revoked.

#### **4.9.3.2 Revocation of a certificate of a PKI component**

In the event of revocation of one of the certificates in the certification chain, the CA informs all concerned holders as soon as possible and by any means (and if possible in anticipation) that their certificates are no longer valid.

Procedures to be implemented in the event of revocation of a certificate of a component of the PKI are described in the "Termination or Change of a Component of the CA" procedure.

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 33/74 NC: PU
---	--	---

#### **4.9.4 Deadline granted to bearer to make the request of revocation**

As soon as the applicant is aware that one of the possible causes of revocation of his jurisdiction is effective, he must file his request for revocation without delay.

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

##### **4.9.5.1 Revocation of a subscriber's certificate**

The revocation service is available 24 hours a day 7 days a week.

Any request to revoke a subscriber's certificate is processed within a period of less than 24 hours. This time period covers the receipt of the authenticated revocation request until the revocation information is made available to the users.

##### **4.9.5.2 Revocation of a Certificate of a PKI Component**

Revocation of a certificate of a PKI component must be made as soon as an event described in the possible revocation causes for this type of certificate is detected. The revocation of a certificate of signature of the CA Servers (signature of certificates, CRL and / or OCSP replies) is carried out immediately, especially in the case of compromise of the key.

#### **4.9.6 Revocation checking requirement for certificate users**

The CU must check the status of the certificates throughout the corresponding certification chain prior to its use and in particular when the certificates involve legal effects. The method used (CRL, OCSP) is at the discretion of the user according to their availability and the constraints related to its application.

The validity of a CRL is controlled by verification of its signature and verification of the validity of the certificate of the CA Servers.

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

The frequency of CRL generation is 24 hours.

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

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 34/74  NC: PU</p>
---	---	--

The publication of a CRL following its generation must be carried out within a maximum of 30 minutes.

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

The NDCA maintains a 24x7 online OCSP server to verify the status of a certificate. There are two instances for the OCSP service:

a. Instance for the verification of the status of the subscribers' certificates:

- The OCSP certificate is issued by the TunServerCA2 authority,
- Certificate revocation information is available on the OSCP server at <http://ocsp.certification.tn:8080>.
- The TunServerCA2 authority publishes and generates a CRL every 24 hours and within half an hour of delay after the revocation of a subscriber's certificate. The validity period of a CRL is 6 days.

B. Instance for verifying the status of the certificate of the subordinate authority:

- The certificate of the OCSP is issued by the authority TunRootCA2,
- The certificate revocation information of authorities issued under TunRootCA2 is available on the OSCP server at <http://ocsp.certification.tn>.
- The TunRootCA2 authority publishes and generates an ARL every 10 months and within 24 hours following the revocation of a subordinate authority certificate. The validity period of an ARL is 365 days.

In both instances, the OCSP server signature certificate contains an id-pkix-ocsp-nocheck extension as defined by RFC 2560.

#### **4.9.10 Online revocation checking requirements for the certificates users**

See section 4.9.6 below.

#### **4.9.11 Other means of information on revocation available**

No other means of getting revocation information is forecasted in this CP / CPS.

#### **4.9.12 Special requirements regarding key compromise**

In the event of a proven or suspected compromise of a private key, revocation of the associated certificate must be requested as soon as possible.

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 35/74 NC: PU
---	--	---

#### **4.9.13 Possible Circumstances for suspension**

The suspension of certificates is not permitted in this CP / CPS.

#### **4.9.14 Who can request suspension**

Not applicable.

#### **4.9.15 Procedure for processing a suspension request**

Not applicable.

#### **4.9.16 Limits on suspension period**

Not applicable.

### **4.10 Certificate status services**

#### **4.10.1 Operational characteristics**

The CA servers provides the CUs with information to enable them to verify and validate, prior to its use, the status of a certificate and the entire corresponding chain of certification (up to and including the Root CA), i.e., to also check the signatures of the chain certificates, the signatures guaranteeing the origin and integrity of the CRL and the status of the Root CA certificate.

CRLs are published on the website of the NDCA available at [crl.certification.tn/TunServerCA2.crl](http://crl.certification.tn/TunServerCA2.crl) and on the directory [ldap.certification.tn](http://ldap.certification.tn) available through the LDAP protocol v3.

#### **4.10.2 Service availability**

The Certificate Status Information feature is available 24 hours a day, seven days a week, without any forecasted interruption.

#### **4.10.3 Optional features**

No optional features available

### **4.11 End of subscription between the subscriber and the CA**

In the event of a contractual, hierarchical or regulatory termination between the CA and the client organization before the end of the certificate's validity, whatever the reason, the latter must be revoked.

 Agence Nationale de Certification Electronique	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 36/74 NC: PU
---	--	---

## 4.12 Key escrow and recovery

The key pair and CA SSL certificates issued in accordance with this CP / CPS are not subject to escrow or recovery.

	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 37/74 NC: PU
---	--	---

## 5 Non-technical security measures

---

### 5.1 Physical security measures

#### 5.1.1 Site geographical location and construction

The PKI's operating site is located at the NDCA. The construction of the site complies with current regulations and standards and takes into account the results of a risk analysis and specific requirements for accidental risks.

#### 5.1.2 Physical access

The infrastructure of the components of the PKI is installed in an enclosure of the NDCA's premises, access to which is controlled and reserved for authorized personnel only. Traceability of access is ensured.

The NDCA has defined a physical security perimeter where the hardware and software of the critical components of the PKI performing the operations of certificate generation and revocation management are installed. The implementation of this perimeter makes it possible to respect the separation of the roles of trust as foreseen in this CP / CPS.

Outside working hours, security is reinforced by the implementation of physical and logical intrusion detection means.

If unauthorized persons are to enter the premises, they are taken over by an authorized person who supervises them. These persons must be permanently accompanied by authorized personnel.

#### 5.1.3 Power and air conditioning

Electricity generation and protection systems are implemented by the NDCA to ensure the availability of computer systems at the PKI main site.

The characteristics of the power supply and air conditioning equipments make it possible to respect the conditions of use of the equipment of the PKI as set by the NDCA and their suppliers. They also allow compliance with the requirements of this CP / CPS, as well as commitments made by CA, regarding the availability of its functions, including revocation management and certificate status information.

#### 5.1.4 Water Exposures

The means of preventing water damage make it possible to respect the requirements of this CP / CPS, as well as the commitments made by the CA, regarding the availability of its functions, in particular the revocation and information management functions and certificate status information.



 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 38/74 NC: PU
---	--	---

### 5.1.5 Fire Prevention and Protection

The fire prevention and fire-fighting measures implemented by the NDCA make it possible to comply with the requirements of this CP / CPS, as well as the commitments made by the CA, regarding the availability of its functions; in particular, the functions of revocation management, publication of information on the validity status of certificates.

### 5.1.6 Media Storage

The means of preserving the information media implemented by the NDCA make it possible to comply with the requirements and commitments made by the CA in this CP / CPS. In the context of the risk analysis, the media and the various information involved in the activities of the PKI have been identified and their security needs defined in terms of data availability, confidentiality and integrity, in particular those stored in the logs, archives and software used by the CA. Details of the classification of this information are established at the level of the property classification procedure.

The media (paper, hard disk, diskette, CD, etc.) corresponding to these information are processed and stored in a secure enclosure accessible only to authorized persons.

### 5.1.7 Waste Disposal

In order to avoid any loss of confidentiality, mechanisms for the destruction of papers (such as shredders) and magnetic information media are implemented at the PKI's operating site and made available to personnel of confidence.

The storage media (hard drive) of the CA are not re-used for any other purpose until the information related to the CA that it is likely to contain is completely destroyed.

At the end of life, the supports are destroyed.

### 5.1.8 Off-Site Backup

The CA performs offsite backups that enable a rapid recovery of PKI services following the occurrence of a disaster or event that seriously and permanently affects the performance of its services. The details of the procedures for safeguarding information are provided in the backup procedure.

## 5.2 Procedural Security Measures

### 5.2.1 Trusted Roles

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 39/74 NC: PU
---	--	---

Those with a trusted role of the PKI are all authorized persons of the NDCA and they know and understand the implications of the operations on which they are responsible. Following the separation of critical tasks, the CA's trust roles are distinguished into five groups:

- Administrative staff, whose responsibility is the technical administration of the components of the PKI;
- Operational staff, whose responsibility is to implement the PKI functions;
- Audit staff, whose responsibility is to carry out the verification of the proper application of the measures and the coherence of operation of the PKI component;
- Security personnel, whose responsibility is to implement the information systems security policy, in particular, the management of physical controls to the equipment of the component systems and the analysis of the event logs in order to detect any incident, anomaly, attempt of compromise, or other event;
- Secrets and activation data holders.

### **5.2.2 Number of persons required per task**

Several roles can be assigned to the same person, when the accumulation does not compromise the safety of the functions implemented. Depending on the type of operations performed, the number and type of roles and persons who may be required to participate may differ. The procedure for managing the roles and responsibilities of the NDCA defines the number of people required for each operation.

### **5.2.3 Identification and authentication for each role**

Prior to the assignment of roles and the corresponding authorizations, the NDCA performs all the necessary checks of the personnel required to work within the entities operating the CA components.

Each assignment of a role to a staff member of the CA shall be notified in writing. The Security Officer is informed of each appointment.

The controls and checks carried out are described in the procedure for managing the roles and responsibilities of the NDCA and are in accordance with the information systems security policy.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 40/74  NC: PU</p>
---	---	--

### **5.2.4 Roles requiring separation of duties**

Several roles can be assigned to the same person, when the accumulation does not compromise the safety of the functions implemented. The attributions associated with each role are described in the NDCA Roles and Responsibilities Management Procedure and are in line with the information systems security policy.

## **5.3 Security measures regarding the personnel**

### **5.3.1 Required qualifications, skills, and empowerment**

The NDCA ensures that the responsibilities of its staff, who are required to work within the PKI, correspond to their professional skills in accordance with the recruitment procedure.

Each person required to work in the CA is subject to a duty of reserve and confidentiality clauses with respect to the NDCA. He is informed of his responsibilities regarding the services of the PKI and the information systems security policy in force in the CA.

### **5.3.2 Background check procedures**


The NDCA ensures the honesty of its staff who work in the PKI by checking when they are recruited that they have not been convicted of a criminal offense in contradiction with their duties. Persons in a trust role must not suffer from a conflict of interests that is prejudicial to the impartiality of their duties.

### **5.3.3 Initial Training requirements**

The PKI staff has already been trained on the internal software, hardware and internal operating and security procedures implemented in accordance with the recruitment procedure. The personnel have knowledge and are deemed to have understood the implications of the operations for which they are responsible.

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

The concerned staff receives adequate information and training prior to any evolution in systems, procedures and organization, depending on the nature of these evolutions. The CA draws up annually a training plan in accordance with the training procedure. The CA maintains evaluation sheets for all training activities carried out.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 41/74 NC: PU</p>
---	---	--

### 5.3.5 Job rotation frequency and sequence

Any rotation of CA staff must not interfere with the continuity and security of services.

### 5.3.6 Sanctions for unauthorized actions

The NDCA decides on the sanctions to be applied when staff abuse their rights or perform an operation that is not in conformity with their duties in accordance with the NDCA's staff regulations.

### 5.3.7 Independent Contractor Requirements

The NDCA does not benefit from the services of contractual employees for the trust roles defined in section § 5.2.1.

In the case of a service provision of external suppliers in the PKI areas, the NDCA information system security policy describes the physical access modality of such a service.

### 5.3.8 Documentation Supplied to Personnel

Staff have adequate documentation of the operational procedures and the specific tools that it implements, as well as the general policies and practices of the PKI components.

The appropriate documentation, which must be available to the staff according to their need to know for the fulfillment of their mission, is composed of at least the following documents:

- The NDCA's staff regulations;
- The security charter;
- The CP / CPS;
- The information system security policy;
- Internal procedures and operating manuals;
- Technical documents relating to the hardware and software used.

## 5.4 Audit Logging Procedures

Event logging involves recording events manually or electronically by input or by automatic generation.

### 5.4.1 Types of Events Recorded

The PKI logs events related to the systems related to the functions they perform under the PKI:

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 42/74 NC: PU
---	--	---

- Creation / modification / deletion of user accounts (access rights) and corresponding authentication data (passwords, certificates, etc.);
- Starting and shutting down computer systems and applications;
- Logging events: Starting and stopping logging, changing logging settings, actions taken following a logging failure;
- Logging / logging off users with trusted roles, and unsuccessful attempts.

Other events are also gathered. These are security events that are not automatically generated by the systems implemented:

- Physical access to sensitive areas;
- Maintenance and system configuration changes;
- Changes to staff with trusted roles;
- Actions to destroy and reset media containing confidential information (keys, activation data, personal information about Users, ...).

In addition to these logging requirements common to all components and functions of the PKI, events specific to the various functions of the PK are also logged:

- Receipt of a certificate request (initial and renewal);
- Validation of a certificate request;
- Events related to signature keys and CA certificates (generation (key ceremony), backup / recovery, destruction, ...);
- Generation of certificates;
- Transmission of certificates;
- Publication and updating of CA-related information;
- Generation of status information for a subscriber's certificate.

The PKI records all events related to the services and protection of the CA it implements. The recordings of events in a log contain at least the following information:

- the type of event;
- the identifier of the one that executed the action and / or the reference of the system triggering the event;
- the date and time of the event;

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 43/74  NC: PU</p>
---	---	--

- the result of the event.

Depending on the event type, the recordings will also include the following fields:

- the recipient of the transaction;
- the name of the requestor of the operation or the reference of the system making the request;
- the name of the persons present (in the case of a transaction requiring more than one person);
- the cause of the event;
- any information featuring the event.

Logging operations are performed in the background throughout the life of the PKI. The accountability of an action rests with the person, component or system that performed it.

#### **5.4.2 Frequency of processing log**

The content of the event logs is analyzed on a regular basis by the CA. The frequency of processing event logs is described in the NDCA event logging procedure.

#### **5.4.3 Retention Period for Audit Log**

Details on how long the event logs are kept are provided in the procedure for logging the NDCA events.

#### **5.4.4 Protection of Audit Log**

Logging is designed and implemented to minimize the risk of circumventing, modifying, or destroying event logs. Integrity checking mechanisms allow the detection of any changes, voluntary or accidental, to these logs.

Event logs are protected on availability (against partial or total loss or destruction, voluntary or otherwise).

Defining the sensitivity of event logs depends on the nature of the information processed and the function. The procedure for logging the NDCA's events and the system documentation specify the means of protection used.

#### **5.4.5 Audit Log Backup Procedures**

The PKI implements the required measures to ensure the integrity and availability of event logs in accordance with the requirements of this CP / CPS and the results of the risk analysis performed.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 44/74  NC: PU</p>
---	---	--

The NDCA's "event logging procedure" specifies the backup measures for event logs.

#### **5.4.6 Event Log Collection System**

Each component of the PKI is responsible for the collection of event logs relating to it.

#### **5.4.7 Evaluation of vulnerabilities**

All components of the CA are able to detect any attempt to violate the integrity of their operation. Logs are analyzed at least once a quarter. This analysis makes it possible to check the concordance between dependent events and help to reveal any anomaly. More details are to be found in the procedure for logging the NDCA's events.

### **5.5 Records archival**

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

The data to be archived are at least the following:

- the CP / CPS;
- complete records of requests to create and revoke certificates;
- Certificates and CRLs as issued or published;
- the event logs of the various components of the PKI;
- computer equipment and software configuration files.

The inventory of the data to be archived is included in the archiving procedure.

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

Subscribers' and CAs' certificates as well as the CRLs and ARLs are archived 20 years after their expiry. The event logs discussed in section 5.4.1 are archived for seven (7) years after their generation.

For the archiving of logs other than the event logs discussed in section 5.4.1, no requirement is stipulated.

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

The archives are protected in integrity and accessible to the authorized persons during the whole time of their preservation.

The means and measures implemented to ensure the protection of archives are specified in the NDCA archiving procedure.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 45/74  NC: PU</p>
---	---	--

#### **5.5.4 Archive backup procedure**

The principles for backing up archives are described in the NDCA's archiving procedure.

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

All components of the CA are regularly synchronized with a Network Time Protocol (NTP) server.

#### **5.5.6 Archive collection system**

The system ensures the collection of records in accordance with the data protection security level (see § 5.5.3).

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

The archives (paper and electronic) are accessible to authorized persons within a maximum of three (3) working days delay.

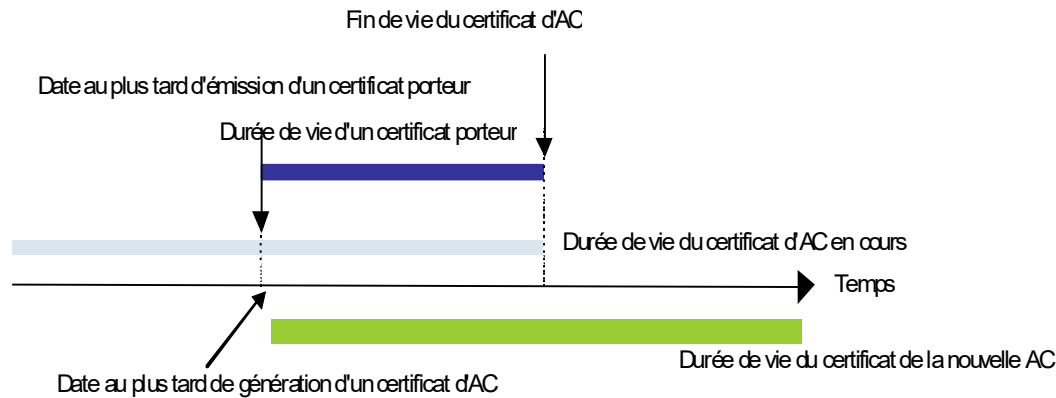
### **5.6 Changing the CA Key**

#### **5.6.1 Certificate of CA**

The CA can not generate a certificate whose expiry date would be later than the expiry date of the CA's key pair. For this purpose, the period of validity of the CA certificate is higher than that of the certificates it signs.

Once a new CA private key has been generated for the CA and a CA certificate has been obtained by the CA of a higher level, it is used from the beginning of the CA period of validity of this certificate to generate new subscribers' certificates and CA CRLs for these new certificates. The previous CA certificate remains valid to validate the certificate path of the old subscribers' certificates issued by the previous CA private key until all subscribers' certificates issued using this key pair expire. The old CA key is then used to sign CRLs for certificates issued under this old CA key.





A CA key can be renewed in advance if:

- the size of a CA key is insufficient to resist progress in breaking the keys;
- the hashing algorithm used to generate certificates or CRLs is found to be of insufficient resistance to resist collisions.

### 5.6.2 Subscriber's Certificate

The lifetime of the holders' certificates is two (2) years at most.

## 5.7 Compromise and disaster recovery

### 5.7.1 Incident and compromise handling procedures

Procedures and means for reporting and dealing with incidents are implemented by the CA, in particular through the analysis of the various event logs.

Through staff awareness and training, these procedures are regularly applied at the level of each CA component to detect the event that triggers a major incident, such as loss, suspicion of compromise, compromise, theft of the CA private key.

In the event of a disaster, the PKI has a recovery plan, which takes account of the disaster scenarios, specifying the triggers and the persons responsible for this plan.

### 5.7.2 Recovery procedures in case of corruption of Computing Resources (hardware, software and/or data)

The CA has a business continuity plan to meet the availability requirements of the various functions resulting from this CP / CPS, the CA's commitments in this CP / CPS and the results of the risk analysis, in particular regarding publication-related functions and / or revocation of certificates.

This continuity plan is tested at least once a year.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 47/74 NC: PU</p>
---	---	--

### 5.7.3 Entity Private Key Compromise Procedures

If the CA signing key is compromised, lost, destroyed, or suspected of being compromised, the NDCA decides, after investigation of the event, to request the higher level CA to revoke the CA certificate. Then, a new CA key pair is generated and a new CA certificate is issued. PKI staff and holders are notified as soon as the former CA certificate is revoked and are immediately informed of the CA's ability to generate certificates. The Business Continuity Plan provides more details about this section.

### 5.7.4 Business continuity capabilities after a disaster

The Disaster Recovery Plan deals with Business Continuity as described in Section 5.7.1. The Business Continuity Procedure scenarios specify the business continuity capabilities of the CA components.

## 5.8 CA Termination

The end of life of the CA is either a partial transfer of activity to another entity or a complete cessation of activity.

The transfer of activity is defined as the end of activity of a component of the CA that does not affect the validity of the certificates issued prior to the transfer concerned and the resumption of this activity organized by the collaborating CA with a new entity.

Cessation of activity is defined as the end of activity of a component of the PKI that affects the validity of certificates issued prior to the cessation concerned.

### 5.8.1 Transfer of Activity

In order to ensure a constant level of confidence during and after the transfer of activity, the CA commits to:

- immediately notify the holders and users of certificates of the proposed changes;
- Establishing procedures to ensure constant service, particularly with regard to archiving (including archiving of subscribers' certificates and certificate information);
- ensure the continuity of the revocation (taking into account a revocation request and publication of the CRL), in accordance with the availability requirements for its functions defined in the CP / CPS.

### 5.8.2 Termination of Activity

The cessation of activity may be total or partial, typically, cessation of activity for a given family of certificates only.

In the event of a partial cessation of activity, the CA agrees to:

- informing the bearers and users of certificates (UC) in advance via the PS;

 Agence Nationale de Certification Electronique	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 48/74 NC: PU
---	--	---

- continue to ensure the revocation of certificates and the publication of CRLs in accordance with the commitments made in this CP / CPS, as long as holders are equipped with new certificates, and at the latest until the end of validity of the last issued certificate.

In the event of a complete cessation of activity, the CA or, in the event of impossibility, any entity which is substituted for it by virtue of a law, regulation, court decision or of an agreement previously entered into with that entity, undertakes to:

- notify holders and users of certificates via the PS or any other means;
- revoke all certificates issued by the CA;
- provide subscribers with tools that enable the detection of revoked certificates;
- refrain from transmitting private keys to anyone to issue certificates or CRLs;
- destroy private keys and all backup copies of private keys that have allowed it to issue certificates or CRLs.

More details are provided in the procedure of termination or changing the components of the CA.

 Agence Nationale de Certification Electronique	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 49/74 NC: PU
---	--	---

## 6 Technical Security Controls

---

### 6.1 Key pair generation and installation

#### 6.1.1 Key pair generation

##### 6.1.1.1 CA keys

The generation of CA signing keys is performed in a secure environment.

The CA signing keys are generated during a key ceremony using a hardware cryptographic resource that complies with the security level requirements (FIPS 140-2 level 3).

The cryptographic devices used for the generation of CA keys use a random number generator (RNG) as defined in the corresponding technical specifications.

During these ceremonies, all operations are performed under perfectly controlled circumstances by personnel in trusted roles by following predefined scripts.

Key ceremonies are conducted at the NDCA premises under the supervision of at least two persons with trust roles and in the presence of witnesses of whom at least two are external to the CA and are impartial. The witnesses attest, in an objective and factual manner, the progress of the ceremony in relation to the script previously defined.

The manipulations of the PIN codes and of the authentication codes are carried out in an environment protected against the risks of leakage of information by video surveillance.

##### 6.1.1.2 Keys generated by keys' holders

The holders of the server certificates generate a cryptographic key whose public key is contained in a PKCS # 10 certificate request supplied to the CA Server.

#### 6.1.2 Private key delivery to subscriber

##### 6.1.2.1 CA Private Key

The private key of the CA is owned by the NDCA. It is generated and protected at the level of a cryptographic module located in the secure premises of the NDCA.

##### 6.1.2.2 Private keys of the carrier

The CA does not generate the private key of the bearers.

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 50/74 NC: PU
---	--	---

### 6.1.3 Public key delivery to the CA

The public key of a bearer is protected in integrity and its origin is authenticated when it is transmitted to and from the CA Servers.

The requestor must generate the SSL certificate request and send it to the NDCA in pkcs # 10 format. Typically, the client generates its query using the key generation tools available on its server.

### 6.1.4 CA public key delivery to certificate users

The certificate of the CA Servers and the footprint of this certificate are published on the NDCA website: <http://www.certification.tn/pub/TunServerCA2.crt>.

This certificate is issued by the NDCA's Root CA, whose self-signed certificate is published on the NDCA's website: <http://www.certification.tn/pub/TunRootCA2.crt>.

The General Terms of Use available are published on the NDCA website: <http://www.certification.tn/rpa>.

### 6.1.5 Key sizes

#### 6.1.5.1 CA Certificate

The recommendations of the relevant national and international bodies (concerning key lengths, signature algorithms, hashing algorithm ...) are periodically consulted in order to determine whether the parameters used in issuing CA certificates should or should not be modified .

The RSA algorithm with SHA-256 hash function is used. The size of the CA servers' key pairs is 4096 bits.

#### 6.1.5.2 Subscriber's certificate

The recommendations of the relevant national and international bodies (concerning key lengths, signature algorithms, hashing algorithm ...) are periodically consulted in order to determine whether the parameters used in issuing bearer's certificates should or should not be modified.

The RSA algorithm with SHA-256 hash function is used for carriers' certificates. The size of the key pairs is 2048 bits.

### 6.1.6 Public key parameters generation and quality checking

The equipment used for the generation of the CA key pairs are cryptographic hardware resources certified FIPS140-2 level 3.

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 51/74 NC: PU
---	--	---

### 6.1.7 Key usage purposes

The use of a CA private key and the associated certificate is strictly limited to the signature of certificates and CRL.

The use of the carrier's private key and the associated certificate is strictly limited to authentication and the establishment of TLS / SSL secure sessions. The use of the "keyUsage" field in the bearer certificate is "digital signature" and "key encipherment" according to the IETF RFC 5280.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic module standards and controls

#### 6.2.1.1 CA Cryptographic Modules

The CA has FIPS 140-2 Level 3 cryptographic modules that provide key protection with a level of security that is considered acceptable against threats to the integrity, availability and confidentiality of key pairs.

The hardware cryptographic resources of the CA use random generators that conform to the state of the art, and the standards in force. The algorithms used to generate the starting hazard are in accordance with current standards.

#### 6.2.1.2 Devices for authentication and signature of bearers

Not applicable.

### 6.2.2 Private key control by multiple persons

The control of private CA signing keys is performed by trusted personnel using the M of N authentication method (3 of 8).

The initialization of the cryptographic modules is controlled via the implementation of a process of sharing of the secrets where the operators of trust intervening must authenticate.

### 6.2.3 Private key escrow

Neither the private keys of CA nor the private keys of the bearers are sequestered.

### 6.2.4 Private key backup

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 52/74 NC: PU
---	--	---

#### **6.2.4.1 CA private key**

Backup copies of private keys are made using hardware cryptographic resources. The CA key pair is backed up under the control of several trusted staff members for availability purposes. CA private key backups are stored in hardware cryptographic resources.

Backups are quickly transferred to a secure, off-site backup site to provide and maintain the CA recovery capability.

#### **6.2.4.2 Private keys of the bearers**

The private keys of the bearers are not the subject of any back-up copy.

#### **6.2.5 Private key archival**

The private keys of the CA are not archived.

The private keys of the bearers are not archived, either by the CA or by any of the components of the PKI.

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

Any transfer of a private key from the CA to / from the cryptographic module for restoration or backup purposes is done in encrypted form by means of the associated cryptographic module.

#### **6.2.7 CA private key storage on cryptographic module**

The private keys of the CA are stored in hardware cryptographic resources, meeting at least the requirements of the level of security considered. The stored private keys are protected with the same security level as the one in which they were generated.

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

##### **6.2.8.1 CA private keys**

The activation of private keys of CA in a cryptographic module is controlled via activation data and initially involves at least three secret holders in trusted roles.

##### **6.2.8.2 Private keys of the bearers**

Not applicable.

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

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 53/74  NC: PU</p>
---	---	--

### 6.2.9.1 CA private keys

Disabling CA private keys in a cryptographic module is automatic as soon as the module is stopped or disconnected.

Cryptographic resources are stored in a secure area to prevent unauthorized manipulation by non-strongly authenticated roles.

### 6.2.9.2 Private keys of the bearers

Not applicable.

## 6.2.10 Method of destroying private key

### 6.2.10.1 CA private keys

A private key of a CA is destroyed at the end of life of this private key, normal or anticipated; in particular, when the corresponding certificate has expired or been revoked.

The authorization to destroy a private key of a CA and the corresponding method are described in the "procedure of termination or changing the components of the CA"

Destruction of a private key involves the destruction of backup copies, activation data, and any elements that can be used to reconstruct it.

### 6.2.10.2 Private keys of the bearers

At the end of the private key's life, the SCR commits to destroy the private key.

## 6.2.11 Cryptographic Module and devices Rating

See Section 6.2.1.

## 6.3 Other aspects of key pair management

### 6.3.1 Public keys archival

The public keys of the CA and the subscribers are archived as part of the archiving of the corresponding certificates.

The means and measures implemented to ensure the protection of archives are specified in the NDCA's archiving procedure.

### 6.3.2 Certificates and key pair lifetimes



 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 54/74 NC: PU
---	--	---

The operational lifetime of a certificate is limited by its expiry or revocation. The operational lifetime of a key pair is equivalent to that of the certificate to which it corresponds. The CA Servers cannot issue carrier's certificates with a lifetime greater than its certificate (see § 5.6).

## 6.4 Activation data

### 6.4.1 Activation data generation and installation

#### 6.4.1.1 Generation and installation of the activation data corresponding to the private key of the CA

The generation of the activation data making it possible to initialize a cryptographic module is carried out according to a schema of M out of N type, in the initialization and customization phase of this module during the key ceremonies (see § 5.2.1) .

These activation data are chosen and entered by the persons responsible for the data themselves. These activation data are only known by those responsible identified by the roles assigned to them and which are detailed in the document "Ceremony of the keys of the root certification authority in the NDCA's PKI". Activation data holders are authorized persons for this trust role.

#### 6.4.1.2 Generation and installation of the activation data corresponding to a private key of the bearer

Not applicable.

### 6.4.2 Activation data protection

#### 6.4.2.1 Protection of activation data corresponding to the private keys of the CA

Activation data is protected from disclosure by a combination of cryptographic mechanisms and physical access control. The holders of activation data and secrets are responsible for their management and protection. A secret holder cannot hold more than one activation data of the same key of CA at the same instant.

#### 6.4.2.2 Protection of the activation data corresponding to the private keys of the subscribers

Not applicable.

### 6.4.3 Other aspects of activation data

Not applicable.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 55/74  NC: PU</p>
---	---	--

## 6.5 Computer security controls

The NDCA has carried out a risk analysis to determine the safety objectives to cover the business risks of the entire PKI and the corresponding technical and non-technical safety measures to be implemented. The ISSP was developed based on this analysis.

### 6.5.1 Specific computer security technical requirements

A minimum level of security assurance offered on the IT infrastructure of the PKI components is defined in the ISSP. The latter meets the following safety objectives:

- identification and authentication of users for access to the system;
- management of usage sessions (disconnection after a period of inactivity, file access controlled by role and user name);
- protection against computer viruses and all forms of compromising or unauthorized software and software updates;
- management of user accounts, including modification and deletion of access rights;
- protecting of the network against intrusions and ensuring confidentiality and the integrity of the data transiting it;
- Audit functions.

The confidentiality and integrity protection of private or secret keys of infrastructure and control is subject to special measures, arising from the risk analysis. Monitoring devices and procedures for auditing the system settings are set up.

### 6.5.2 Computer systems rating

Security measures for the PKI are based on a risk analysis. The cryptographic module implemented has been certified FIPS 140-2 level 3.

## 6.6 System development controls

The system development controls are as follows:

- software and hardware are acquired in a manner that it reduces the possibilities for a particular component to be altered;
- The developed software has been developed in a controlled environment, and the developing process is defined and documented. Software to which this requirement does not apply is acquired from authorized sources;
- the hardware and software dedicated to the PKI are not used for other activities other than the CA's;

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 56/74  NC: PU</p>
---	---	--

- CA software is subject to a search for malicious codes prior to first use and periodically thereafter;
- Hardware and software updates are installed by trusted and trained personnel according to the procedures in force.

### 6.7.1 Security Management Measures

The configuration of the CA system, as well as any changes or developments, is documented and monitored by the CA. Any unauthorized modification of the software or configuration of the CA is detected by implemented mechanisms.

A formal configuration management method is used for the installation and subsequent maintenance of the CA system. When first loaded, it is ensured that the software of the CA is the one delivered by the vendor, and that it has not been modified before being installed, and that it corresponds to the desired version .

### 6.7.2 Systems' life cycle security rating

For the software and hardware evaluated, the CA continues to monitor the maintenance process requirements to maintain the level of trust.


## 6.8 Network security controls

The CA is online accessible through computer stations under control. The accessible components of the PKI are connected to the Internet in an appropriate architecture with security gateways and provide continuous service (except during maintenance or backup).

The other components of the CA PKI use appropriate security measures to ensure that they are protected against denial-of-service and intrusion attacks. These measures include the use of firewalls and filter routers. Unused ports and network services are disconnected. Any flow control device used to protect the network on which the PKI system is hosted refuses any service except those required by the PKI system, even if those services are capable of being used by other devices on the network.

The LAN equipment used by the CA is maintained in a physically secure environment and its configurations are periodically audited to verify compliance with the requirements specified by the CA.

## 6.9 Time-Stamping

 Agence Nationale de Certification Electronique	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 57/74 NC: PU
---	--	---

All components of the CA are regularly synchronized using an NTP (Network Time Protocol) server. The time provided by this time server is used in particular to establish a safe dating of:

- the validity of a subscriber's certificate;
- the beginning of revocation of a subscriber's certificate;
- the registration of events in logs.

	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 58/74 NC: PU
---	--	---

## 7 Certificates and CRL profiles

This chapter discusses requirements for profiles of X.509 v3 certificates of the CA or issued by it, as well as the CRL profiles. Certificates issued in accordance with this CP / CPS comply with RFC 5280.

### 7.1 Certificate profile

Certificates issued by the CA Servers are certificates in X.509 v3 format. The CA and subscriber's certificate fields are defined in RFC 5280.

#### 7.1.1 Certificate of CA

The main information contained in the certificate of the CA Servers are:

Basic Field	Value
Version	2 (= version 3)
Serial Number	128 bit
Issuer	C=TN O=National Digital Certification Agency CN=Tunisian Root Certificate Authority – TunRootCA2
Not Before	Beginning of the period of validity of the certificate
Not After	End of the period of validity of the certificate
Subject	C=TN O=National Digital Certification Agency CN=Tunisian Server Certificate Authority – TunServerCA2
Subject Public Key	Public key of CA Servers
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

Extensions

Basic Field	Criticality	Value
Key Usage	Critical	Certificate Sign and CRL Sign
Certificate Policies	non critical	Policy: 2.16.788.1.2.6.1.8 CPS: <a href="https://www.certification.tn/cps">https://www.certification.tn/cps</a>

 <small>Agence Nationale de Certification Electronique</small>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 59/74 NC: PU
--	--	---

Basic Field	Criticality	Value
		User Notice: Organization: National Digital Certification Agency Number: 1 Explicit Text: <a href="https://www.certification.tn/rpa">https://www.certification.tn/rpa</a>
Authority Information Access	non-critical	OCSP : <a href="http://ocsp.certification.tn">http://ocsp.certification.tn</a> Certificate of Issuing CA : <a href="http://www.certification.tn/pub/TunRootCA2.crt">http://www.certification.tn/pub/TunRootCA2.crt</a>
Basic Constraints	Critical	CA:TRUE, pathlen:0
Crl Distribution Points	non critical	Specifies the HTTP address where the CRL is published : <a href="http://crl.certification.tn/TunRootCA2.crl">http://crl.certification.tn/TunRootCA2.crl</a>

### 7.1.2 Subscriber's Certificate

The main information contained in the holder's certificate is:

Basic Field	Value
version	2 (=version 3)
Serial Number	Defined by the tool
issuer	C=TN O=National Digital Certification Agency CN=Tunisian Server Certificate Authority – TunServerCA2
Not Before	Beginning of the period of validity of the certificate
Not After	End of the period of validity of the certificate
subject	C=(Required) O= (Required) OU= (Optional) CN=(Required) Email= (Optional) L = (Required)
Subject Public Key	Holder's public key

 Agence Nationale de Certification Electronique	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 60/74 NC: PU
---	--	---

Basic Field	Value
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

### Extensions

Basic Field	Criticality	Value
Subject Alternative Name		At least one entry containing the FQDN.
Key Usage	critical	Authorized uses of the private key Digital Signature, Key Encipherment
Extended Key Usage	non critical	Other authorized uses: TLS Web server authentication, TLS Web client authentication
Authority Information Access	non critical	OCSP : <a href="http://ocsp.certification.tn:8080">http://ocsp.certification.tn:8080</a> Certificate of the issuing CA: <a href="http://www.certification.tn/pub/TunServerCA2.crt">http://www.certification.tn/pub/TunServerCA2.crt</a>
Basic Constraints	critical	CA:FALSE
Crl Distribution Points	non critical	Specifies the HTTP address where the CRL is published: <a href="http://crl.certification.tn/TunServerCA2.crl">http://crl.certification.tn/TunServerCA2.crl</a>
Certificate Policies	non critical	Policy: 2.16.788.1.2.6.1.8 CPS: <a href="https://www.certification.tn/cps">https://www.certification.tn/cps</a> User Notice: Organization: National Digital Certification Agency Number: 1 Explicit Text: <a href="https://www.certification.tn/rpa">https://www.certification.tn/rpa</a>

### 7.1.3 OCSP Certificate

The main information contained in the certificate of the OCSP answering machine is:

Basic Field	Value
version	2 (=version 3)
Serial Number	Defined by tool
issuer	C=TN O=National Digital Certification Agency CN=Tunisian Server Certificate Authority – TunServerCA2

 Agence Nationale de Certification Electronique	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 61/74 NC: PU
---	--	---

Basic Field	Value
Not Before	Beginning of the period of validity of the certificate
Not After	End of the period of validity of the certificate
subject	C=(Required) O= (Required) OU= (Optional) CN=(Required) Email= (Optional) L = (Required)
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

### Extensions

Basic Field	Criticality	Value
Subject Alternative Name		At least one entry containing the FQDN.
Key Usage	critical	Digital Signature
Extended Key Usage	non critical	OCSP Signing
Authority Information Access	non critical	Certificate of the issuing CA: <a href="http://www.certification.tn/pub/TunServerCA2.crt">http://www.certification.tn/pub/TunServerCA2.crt</a>
Basic Constraints	critical	CA:FALSE
Crl Distribution Points	non critical	Specifies the HTTP address where the CRL is published: <a href="http://crl.certification.tn/TunServerCA2.crl">http://crl.certification.tn/TunServerCA2.crl</a>
Certificate Policies	non critical	Policy: 2.16.788.1.2.6.1.8 CPS: <a href="https://www.certification.tn/cps">https://www.certification.tn/cps</a> User Notice: Organization: National Digital Certification Agency Number: 1 Explicit Text: <a href="https://www.certification.tn/rpa">https://www.certification.tn/rpa</a>

## 7.2 CRL profile

CRL features are :



 Agence Nationale de Certification Electronique	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 62/74 NC: PU
---	--	---

Basic Fields	Value
version	1 (= version 2)
signature	sha256WithRSAEncryption OID:1.2.840.113549.1.1.11
issuer	C=TN O=National Digital Certification Agency CN=Tunisian Server Certificate Authority – TunServerCA2
This Update	UTC date and time of the generation of the CRL
Next Update	UTC date and time of the CRL update
Revoked Certificates	List of serial numbers of revoked certificates and their date of revocation

### Extensions

Basic Fields	Criticality	Value
Crl Number	non critical Extension	Incremented integer

### Other Features :

<b>Features of a CRL :</b>	Validity period: 6 days Frequency of update: 24h
----------------------------	---

## 7.3 OCSP profile

The CA Servers operates an OCSP responder in accordance with RFC 2560 and RFC5019.

### 7.3.1 Version Number

The OCSP responder operates in version 1

### 7.3.2 OCSP Extension

No provision.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 63/74  NC: PU</p>
---	---	--

## 8 Compliance Audit and Other Assessments

This chapter deals with the audits and assessments under the NDCA's responsibilities.

The CA Servers must be integrated into the NDCA internal audit plan.

The purpose of these audits is to validate the proper functioning of its PKI and validate the conformity of the implementation, use and operation of the CA as described in the CP / CPS; as well as in the ETSI TS 102 042 standard.

An audit may also have as a purpose checking the absence of corruption or impairment of the CA's services and data, and the absence of vulnerabilities on its services, that can be exploited to achieve such corruptions.

### 8.1 Frequency or circumstances of assessment

As part of the ETSI qualification, the CA Servers is periodically audited for compliance at least once a year.

Control audits can be performed periodically or when the NDCA receives suspicious information about the security of the CA servers.

In addition, following any major changes in its PKI, the NDCA must organize a compliance audit.

### 8.2 Identity/qualifications of assessors

The checking of a component is carried out by a team of auditors that are competent in the security of information systems and in the field of activity of the audited component. The audit team may be internal or external to the NDCA.

### 8.3 Relationship between the assessors and the assessed entity

The audit team does not belong to the entity operating the audited component, regardless of this component. It is duly authorized to carry out the checks in question. If the entire CA is checked, the audit team should not be part of the operational divisions of the CA.

### 8.4 Topics covered by assessment

Compliance checks are carried out on a component of the PKI (spot checks) or on the whole PKI architecture (periodic inspections) and are intended to verify compliance with the commitments and practices defined in this CP / CPS , as well as the resulting elements (operational procedures, resources implemented, etc.).

 Agence Nationale de Certification Electronique	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 64/74 NC: PU
---	--	---

## 8.5 Actions taken as a result of deficiency

At the end of a compliance check, the audit team gives an opinion to the heads of the CA Servers among the following ones: "success", "failure", "to be confirmed". According to the given opinion, the consequences of the check are as follows:

- In the event of failure, and depending on the extent of the non-conformities, the audit team issues recommendations to the operations manager, which may be the cessation (temporary or permanent) of the activity, revocation of the certificate of the component, the revocation of all the certificates issued since the last positive control, etc. The choice of the measure to be applied is made by the operating manager and must respect its internal security policies.
- In the event of a "To be Confirmed" result, the operations manager provides the component with a notice specifying the time frame within which the non-conformities must be repaired. Then, a "confirmation" check will allow to verify that all the critical points have been solved.
- If successful, the operations manager confirms to the controlled component compliance with the requirements of this CP / CPS.

## 8.6 Communication of results

Following a compliance audit, a compliance verification report, citing the versions of the CP / CPS used for this assessment and, if necessary, including the corrective measures to be applied by the component, shall be handled to the NDCA.

 Agence Nationale de Certification Electronique	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 65/74 NC: PU
---	--	---

## 9 Other Business and Legal Matters

---

### 9.1 Fees

#### 9.1.1 Certificate issuance or renewal fees

The fees conditions in force for the acquisition or renewal of certificates are published on the website <http://www.certification.tn>.

The fees are updated by the board of directors. After a favorable opinion from the latter, the NDCA forwards the proposal to the Ministry for validation.

Prior to the implementation of the new fees, the NDCA undertakes to notify its customers and partners within a minimum of one month by sending them the date of entry into force of these fees.

#### 9.1.2 Certificate access fees

Access to certificates is not the subject of special invoicing by the NDCA.

#### 9.1.3 Revocation or status information access fees

The service for accessing status and revocation information of a certificate, whether using the CRL or the OCSP server, is not the subject of a special invoice from the NDCA.

#### 9.1.4 Fees for other services

Not applicable.

#### 9.1.5 Refund Policy

The NDCA does not reimburse the costs of electronic certificates because the acceptance of any file is made only if the file is complete. An incomplete file is automatically rejected

### 9.2 Financial responsibility

#### 9.2.1 Insurance coverage

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

 <p>Agence Nationale de Certification Electronique</p>	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 66/74 NC: PU
---	--	---

### 9.2.2 Other assets

No Stipulation.

### 9.2.3 Insurance or warranty coverage for end-entities

Not applicable.

## 9.3 Confidentiality of business information

### 9.3.1 Scope of confidential information

The following information (non-exhaustive list) are considered confidential:

- private keys of CA certificates;
- the activation data associated with the cryptographic key pairs;
- technical information relating to the safety of the operation of the cryptographic modules;
- event logs of the CA components;
- audit reports;
- causes of revocation;
- technical information relating to the safety of the operation of certain PKI components.

### 9.3.2 Information not within the scope of confidential information

Information published by the PS is considered non-confidential.

### 9.3.3 Responsibilities to protect confidential information

The CA complies with the legislation in force in Tunisia.

## 9.4 Privacy of personal information

### 9.4.1 Private information protection policy

The NDCA operates its PKI in accordance with the Tunisian legislation in force on the subject.

In particular, according to Organic Law No. 2004-63 of July 27<sup>th</sup>, 2004, Article 27, the holder must consent to the processing of his / her personal data before any use.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 67/74  NC: PU</p>
---	---	--

In addition, according to Article 12, the data collected may not be used by the NDCA or a third party for purposes other than the initial verification of identity and the generation of the certificate, unless the holder explicitly agrees to it, according to the same Law, Chapter IV.

The CA must inform the holder of the procedures he applies in terms of protection of personal data (Article 31).

Finally, the holder has a right to access and modify his personal data according to article 32.

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

Information considered to be of a personal nature are as follows:

- the registration file, including in particular the identification data of the holder;
- reasons for the revocation of the holders' certificates.

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

Not Applicable.

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

All components process and protect all personal data so that only staff in trust roles have access to it, according to this CP / CPS.

Holders have the right to access and rectify their personal data collected by the NDCA for the creation, renewal, recovery and revocation of the certificate.

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

The prior and expressed consent of the certificate holder concerning the use of his personal data is required upon registration. No personal data can be collected without his consent, according to the Organic Law n ° 2004-63 of July 27<sup>th</sup>, 2004, Articles 27 and 12.

The bearer is informed prior to any processing of his personal data of the procedures that the CA Servers applies in terms of protection of the personal data.

#### **9.4.6 Conditions for Disclosure of personal information to judicial or administrative authorities**

The CA acts in accordance with the Tunisian regulations. The NDCA has procedures allowing the access of the judicial authorities to personal data.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 68/74  NC: PU</p>
---	---	--

#### 9.4.7 Other information disclosure circumstances

In the event of a transfer of activity (see § 9.15.2), the holder is asked to agree to the transfer of his / her personal data.

### 9.5 Intellectual and industrial property rights

All intellectual property rights held by the NDCA are protected by applicable law, regulations and other international conventions. They may lead to civil and criminal liability in the event of non-compliance:

- **Law No 2007-50 of July 23<sup>rd</sup>, 2007** amending and supplementing Law No 2001-36 of April 17<sup>th</sup>, 2001 on the protection of trademarks and services.
- **Law No. 2001-58 of June 7<sup>th</sup>, 2001** authorizing the membership of Tunisia to the international treaty on cooperation in the matter of patents.
- **Law No. 2000-84 of August 24<sup>th</sup>, 2000** that clearly defines the terminology used, deals with the right to a patent, the procedure of the patent application, the grant of the patent, the remedies, the rights and obligations arising from the patent, the waiver of nullity and forfeiture, transfer, disposal and seizure of rights; contractual licenses, compulsory licenses, licenses of office, counterfeiting and associated penalties, and lastly border measures.

### 9.6 Representations and warranties

The CA is required to:

- respect and apply this CP / CPS;
- respect the clauses that bind it to the bearers and users of certificates;
- submit to the conformity checks carried out by the auditor appointed by the CA and / or the qualification body.

#### 9.6.1 Certification Authorities

CA Servers is responsible to its customers, certification recipients and third-party users for certification service operations performed by any of the components of the PKI. In particular, the CA Servers undertakes, during the period of validity of the issued carrier's certificate, in a non-exhaustive manner, the following guarantees:

- **Legal existence:** The CA Servers, verifies and confirms that the subject in the certificate, before its generation date, exists legally;
- **Certificate Authorization:** The CA Servers verifies and confirms that the applicant has the necessary rights to represent the organization requesting the certificate;

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 69/74  NC: PU</p>
---	---	--

- Right to use a domain name: CA Servers has taken all reasonable steps to verify that, prior to the date of issuing of the certificate, the subject in the certificate is exclusively entitled to use the domain name listed in the certificate;
- Accuracy of information: The CA Servers has taken all reasonably necessary steps to verify that all information included in the certificate is accurate prior to its generation date;
- No misleading information: The CA Servers has taken all measures reasonably necessary to reduce the likelihood that the information contained in the certificate will be erroneous with the implementation of procedures for the entry and validation of electronic certificate requests;
- Applicant Identity: The CA Servers has taken all reasonably necessary steps to verify the identity of the certificate applicant prior to its generation;
- Applicant's agreement: see section §9.6.3.
- Status: The CA Servers guarantees to maintain an online answering machine on the status of certificates that it issued accessible 24/7;
- Revocation: The CA Servers follows the guidelines for the revocation of a certificate as described in Section 4.9.

In addition, the CA Servers has the obligation to:

- Be able to demonstrate the relationship between a holder and his certificate in accordance with the requirements of § 4 above;
- Protecting CA private keys and their activation data in integrity and confidentiality;
- Guarantee and maintain the consistency of the CP / CPS with the services of the PKI;
- Implement the technical means and employ the human resources necessary for the implementation and realization of the services to which she / he is committed to in the CP / CPS;
- Document internal operating procedures;
- Regularly check the integrity of its services and data;
- Take the necessary measures to correct the non-conformities detected in the audits, within the deadlines recommended by the auditors.

### **9.6.2 Registration service**

The RA of the CA Servers complies with all relevant CA obligations defined in section § 9.6.1 by restricting itself to the services it performs under this CP / CPS.



 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 70/74  NC: PU</p>
---	---	--

### 9.6.3 Certificate holders

Certificate holders must comply with all requirements of this CP / CPS. They shall comply with the following obligations:

- Respect the terms of the contract that bonds him with the CA;
- Ensure that the information provided to the NDCA concerning its identification or that of the identified entity is accurate, complete and that the submitted documents are valid;
- Commitment in case of loss or <sup>2</sup> private key, to request revocation of the certificates as soon as possible.

The General Terms of Use formalizes the relationship between the holder and the CA.

### 9.6.4 Certificate Users

Certificate Users (CUs) must comply with all requirements of this CP / CPS. In particular, they undertake to use software that is able to verify that the certificate:

- is not outside of its period of validity at the time of its use,
- is not revoked,
- is actually used in accordance with the practice prescribed in the certificate

### 9.6.5 Other participants

The CP / CPS does not specify other participants.

## 9.7 Disclaimers of warranties

The CA guarantees through its various services:

- the identification and authentication of the bearers with the certificates generated by the CA;
- management of the corresponding certificates and certificate validity information according to this CP / CPS.

No further warranty can be provided by the CA.

## 9.8 Liability

The NDCA's responsibility is limited to the provision of certificates in accordance with the requirements of this CP / CPS.

The use of the certificates provided is strictly limited to the use cases provided for in this CP / CPS. Under no circumstances can the NDCA be held liable for any breach by a holder or a CU who has been informed of his obligations.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 71/74 NC: PU</p>
---	---	--

In addition, the NDCA cannot be held liable for any damage caused when using a certificate, including:

- Loss of profits;
- Loss of data;
- Indirect or consequential damages arising out of or in connection with the use, delivery, licensing, performance or otherwise of issued certificates or signatures;
- Any other damage except those due to a trust in the verified information contained in the certificates.

The liability of the holder is incurred in the event of an error in the verified information of the certificates resulting from fraud or failure of the holder.

## 9.9 Indemnities

This CP / CPS does not have a requirement in this regard.

## 9.10 Term and anticipated termination of this CP/CPS

### 9.10.1 Term

This CP / CPS must remain in effect at least until the end of the last certificate issued under this CP / CPS.

### 9.10.2 Anticipated Termination of validity

Depending on the nature and extent of the changes made to this CP / CPS, the compliance period will be determined according to the applicable regulations.

Except in exceptional cases related to changes in security requirements, updating of this CP / CPS does not require the early renewal of certificates already issued.

### 9.10.3 Effect of termination and remaining applicable provisions

This CP / CPS does not make any requirements in this regard.

## 9.11 Amendments to the CP/CPS

### 9.11.1 Procedures for amendments

The CA undertakes to check that any proposed amendment to this CP / CPS remains in compliance with the requirements of the ETSI TS 102 042 standard.

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 72/74 NC: PU</p>
---	---	--

### **9.11.2 Mechanism and reporting period for amendments**

There is no provision for systematic and periodic review of this CP / CPS.

In the event of a change, the CA is responsible for assessing the need for an updated CP / CPS. It shall give at least two months notice to the CA components of its proposed amendment before proceeding with the changes and depending on the purpose of the amendment.

### **9.11.3 Circumstances under which an OID is to be changed**

The OID of the CP / CPS is modified at each application of any evolution having a major impact on the certificates already issued.

## **9.12 Conflict Resolution Provisions**

In case of contestation or dispute, any party must notify the NDCA by registered letter with acknowledgment of receipt. The NDCA undertakes to process these notifications and to provide a response within thirty (30) days.

The requests are addressed directly or through a lawyer to the director of the NDCA, by registered letter with acknowledgment of receipt.

The request must contain the following information:

- The name, legal form, registered office of the applicant and, where applicable, the registration number in the trade register,
- The name and registered office of the defendant;
- A detailed statement of the subject matter of the dispute and the requests.
- The application must be accompanied by all documents, correspondence and preliminary evidence.
- The registration office of the agency is responsible for registering the request according to its number and date, in the business register.
- the dispute can be settled amicably.
- If the conciliation attempt fails, the courts of Ariana are competent.

## **9.13 Competent Jurisdictions**

The laws and regulations in force in the Tunisian territory are applied.

## **9.14 Compliance with laws and regulations**

This CP/CPS is subject to the laws and regulations applicable on the Tunisian territory.

## **9.15 Miscellaneous provisions**

 <p>Agence Nationale de Certification Electronique</p>	<p><b>CP/CPS of the Tunisian Server CA PTC BR</b></p>	<p>Code : PL/SMI/07  Version : 07  Date : 27/02/2018  Page : 73/74  NC: PU</p>
---	---	--

### **9.15.1 Global agreement**

The NDCA validates all possible agreements made with the partners.

### **9.15.2 Transfer of business**

See Section 5.8.

### **9.15.3 Consequences of an Invalid Clause**

In the case of an invalid clause of this CP / CPS, the validity of the other provisions is not affected. The CP / CPS continues to apply in the absence of the inapplicable clause while respecting the intent of the parties concerned.

The consequences will be dealt with according to the legislation in force.

### **9.15.4 Application and Waiver**

This CP / CPS does not make any specific requirements on the subject.

### **9.15.5 Force majeure**

The occurrence of irresistible, insurmountable and unpredictable events is considered as force majeure.

The CA shall not be held responsible for any indirect damage or interruption of its services due to force majeure, which would have caused direct damage to the holders.

## **9.16 Miscellaneous provisions**

Not applicable.

 Agence Nationale de Certification Electronique	<b>CP/CPS of the Tunisian Server CA PTC BR</b>	Code : PL/SMI/07 Version : 07 Date : 27/02/2018 Page : 74/74 NC: PU
---	--	---

## 10 References

---

The referenced documents are as follows:

Ref.	Document
[X.509]	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. 6 th Edition. Version of november 2008.  Available at : <a href="http://www.x500standard.com/index.php?n=Ig.LatestAvail">http://www.x500standard.com/index.php?n=Ig.LatestAvail</a> .
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - november 2003.  Available at : <a href="http://www.ietf.org/rfc/rfc3647.txt">http://www.ietf.org/rfc/rfc3647.txt</a>
[ETSI]	European Telecommunications Standards Institute – ETSI TS 102 042 V2.1.1 (2009-05) – Electronic Signatures and Infrastructures (ESI): Policy requirements for certifications authorities issuing public key infrastructures
[BR-PTC]	CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates"