Agence Nationale de Certification Electronique

TUNISIA Mobile ID PKI

Certificate Policy / Certification Practice Statement

Version 01

Table of Contents

1. INTRODUCTION

1.1 Overview

The Agence Nationale de Certification Electronique was founded in accordance with Law n°2000-83 of 9 August 2000 governing electronic exchanges and commerce in Tunisia. The Agence Nationale de Certification Electronique is a government-owned Certificate Authority (CA) and will be referred to in the remainder of this document with its trademark name "TunTrust".

In this document, the words "TunTrust CA", "Mobile ID ROOT CA", "MOBILE ID ISSUER CA" and "Mobile ID PKI" are used interchangeably and include MOBILE ID ROOT CA and Issuing CA of the Agence Nationale de Certification Electronique.

Referred as Certificate Policy and Certification Practice Statement (CP/CPS), this document has been prepared in compliance with the guide book of "IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" for the purpose of describing how TunTrust executes its operations during providing certification services.

This CP/CPS document describes the execution of the services in regard to accepting Certificate applications, Certificate issuance and management, and Certificate revocation procedures in compliance with administrative, technical and legal requirements.

This CP/CPS also determines practice responsibilities and obligations of TunTrust, applicants, Subscribers and relying parties that use or rely on Certificates issued by TunTrust. Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CP/CPS is divided into nine parts that cover the security controls and practices and procedures for Certificate services operated by TunTrust. To preserve the outline specified by RFC 3647, Section headings that do not apply are accompanied with the statement "Not applicable" or "No stipulation" along with a brief explanation of the reason.

1.2 Document Name and identification

This document is the TunTrust CP/CPS followed by the Mobile ID Root CA and its subordinate CA and was approved for publication by the TunTrust Board of Directors. This CP/CPS document is disclosed to the public at the website https://www.tuntrust.tn/repository.

Note: The OID of TunTrust is joint-iso-itu-t(2) country(16) tn(788) public-sector(1) public-sector-enterprises(2) tuntrust(7). The OID of the present document is: 2.16.788.1.2.7.1.3.

Revisions of this document have been made as follows:

Version	Date	Comment	Changes
01	17 October 2023	The original CP/CPS document for public.	The whole document

1.3 PKI Participants

PKI Participants defined within the scope of this document are the parties bearing relevant rights and obligations within the certification services of TunTrust.

These parties are defined as CA, Registration Authority, Subscribers and Relying Parties.

1.3.1 CERTIFICATION AUTHORITY (CA)

The Mobile ID PKI consists of a two-level CA hierarchy and is formed using one issuing CA.

The Mobile ID PKI consists of the following CAs:

- One "MOBILE ID ROOT CA" root-signing the subordinate CA and kept offline.
- One Issuing CA "MOBILE ID ISSUER CA" issued by "MOBILE ID ROOT CA" and operates online to issue Qualified Certificates. TunTrust does not have any third-party Subordinate CAs.

Certificate profiles of Mobile ID PKI are detailed in Appendix A, B and C.

MOBILE ID ROOT CA

MOBILE ID ISSUER CA

2.16.788.1.2.7.1.3.1

End user

2.16.788.1.2.7.1.3.1.1
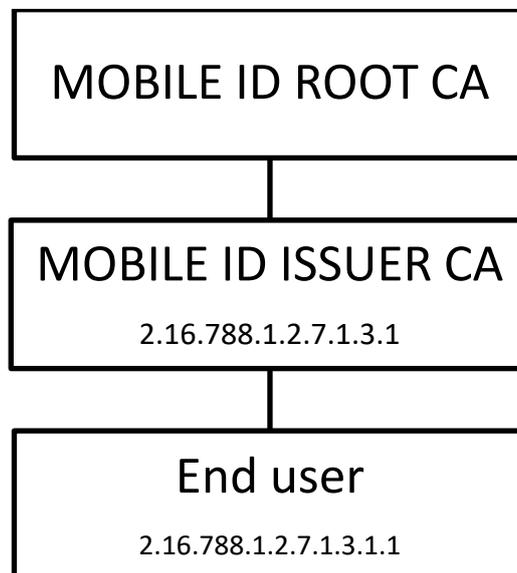
Fig-1: Mobile ID PKI CAs Hierarchy

End User Certificates issued by **MOBILE ID ISSUER CA**:

Service	Description	OID
Mobile-ID	An authentication and digital signing Certificate on a remote QSCD for natural person, that is compliant to ETSI EN 319 411-2.	QCP-n-QSCD OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.7.1.3.1.1 OID: 0.4.0.194112.1.2

1.3.2 REGISTRATION AUTHORITY (RA)

Mobile ID CAs rely on a dedicated network of registration authorities made of:

- a Central Registration Authority (CRA) operated by TunTrust,
- a Delegated Registration Authority (DRA) operated by CNI, and

− a set of Physical Verification Point (PVP) operated by Telecom operators in Tunisia.

TunTrust has a contractual agreement with CNI and Telecom operators which indicates the authorization for their role as RA and PVP and clearly details the minimum requirements, processes and liabilities according to the CP/CPS.

1.3.2.1 THE CENTRAL REGISTRATION AUTHORITY

TunTrust operates a Central Registration Authority (CRA) that registers subscribers of certificates issued by the TunTrust CAs.

The Central Registration Authority is responsible for:

− Accepting, evaluating, approving or rejecting the registration of Certificate applications,
− Requesting issuance of a Certificate via a multi-factor authentication process following the approval of a certificate application,
− Notification of changes in the information supporting the certification process of an end-user,
− Initiating the process to revoke a certificate from the TunTrust CAs,
− Archiving of the registration data.

The CRA interacts indirectly and/or directly with the Subscribers and directly with the CA to deliver certification services.

1.3.2.2 DELEGATED REGISTRATION AUTHORITY (DRA)

TunTrust delegates the performance of its functions to Delegated Registration Authority (DRA) that have to abide by all the requirements of the DRA agreement and this CP/CPS. DRA may, however implement more restrictive practices based on their internal requirements.

The Delegated Registration Authority (DRA) is responsible of:

− Collecting Applicant personal data including full name, date of birth, mobile phone number and national card identifier number,
− Registering Subscribers for certification services,
− Verify that the Applicant submitting the request controls the mobile phone number referenced in the Application form. The mobile phone control is performed through a verification of the couple national card identifier and phone number through APIs provided by telecom operators. In addition, the verification is performed by a challenge-response procedure by sending an SMS OTP to the mobile phone number. The Applicant must respond with the received OTP within a limited time to demonstrate control over that phone number,
− Verify the Applicant data through APIs provided by national registry database,
− Transfer subscribers's data through APIs provided by the CRA,
− Initiating the process to revoke a certificate.

1.3.2.3 PHYSICAL VERIFICATION POINT (PVP)

The PVP is performed by Telecom operators in Tunisia. The physical authentication process must comply to this CP/CPS.

An official list of Physical Verification Points is available under the following URL: https://www.mobile-id.tn.

1.3.3 SUBSCRIBERS

Subscribers are natural persons that successfully apply for and receive a Certificate to support their use in transactions, communications and the application of Digital Signatures.

A Subscriber, as used herein, refers to the Subject of the Certificate. Prior to the verification of identity and issuance of a Certificate, a Subscriber is an Applicant.

Subscribers are responsible for using their certificates in compliance with this CP/CPS.

1.3.4 RELYING PARTY

Any natural person or legal Entity that relies on a valid Certificate issued by a TunTrust CA. Relying parties are responsible for verifying the validity of the Certificates.

To verify the validity of a Certificate, relying parties can refer to the CRL or OCSP response. The locations of the CRL distribution point and OCSP responder are detailed within the Certificate.

1.3.5 OTHER PARTICIPANTS

In the addition to the PKI participants described in Sections1.3.2, **Erreur ! Source du renvoi introuvable.** and 1.3.3, TunTrust will involve other parties as needed.

1.4 Certificate Usage

1.4.1 APPROPRIATE CERTIFICATE USAGE

At all times, participants in the TunTrust PKI are required to use certificates in accordance with this CP/CPS and all applicable laws and regulations.

1.4.2 PROHIBITED CERTIFICATE USES

Certificate use is restricted by using certificate extensions on key usage and extended key usage. Any usage of the Certificate inconsistent with these extensions is not authorized. Certificates shall be used only to the extent the use is consistent with applicable law.

Certificates issued under this CP/CPS do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment on which the certificate has been installed is not free from defect, malware or virus.

1.5 Policy Administration

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

The organization administering the CP/CPS is TunTrust. Its Board of Directors acts as Policy Approval Authority. The Board of Directors is composed of the senior management of TunTrust.

The TunTrust Board of Directors is the high-level management body with final authority and responsibility for:

- Specifying and approving the TunTrust infrastructure and practices.
- Approving the TunTrust CP/CPS.
- Defining the review process for practices and policies including responsibilities for maintaining the CP/CPS.
- Defining the review process that ensures that the TunTrust CAs properly implements the above practices.
- Publication to the Subscribers and Relying Parties of the CP/CPS and its revisions.

1.5.2 CONTACT PERSON

TunTrust Certificate Policy Authority may be contacted at the following address:

> TUNTRUST - Agence Nationale de Certification Electronique
> Policy Authority
> Technopark El Ghazala, Road of Raoued, Ariana, 2083, Tunisia.
>
> Tel.: +216 70 834 600
> Mail: pki@tuntrust.tn
> Web: http://www.tuntrust.tn

Subscribers, Relying Parties, Application Software Suppliers, and other third parties can submit Certificate Problem reports of suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates via email to: revoke@tuntrust.tn. Further details are available in https://www.tuntrust.tn/content/revocation-certificat.

1.5.3 PERSON DETERMINING CP/CPS SUITABILITY FOR THE POLICY

The Policy Authority is responsible for determining the suitability and applicability of this CP/CPS based on the results and recommendations received from a Qualified Auditor as specified in Section 8.

1.5.4 CP/CPS APPROVAL PROCEDURE

TunTrust's Certificate Policy Authority will approve the CP/CPS, along with any amendments. Any amendments made to the CP/CPS will be reviewed by the Policy Authority for consistency with the practices that are implemented prior to its approval. Changes made will be tracked within the revision table. Refer to Section 9.12 for CP/CPS amendment procedure.

1.6 Definitions and Acronyms

1.6.1 DEFINITIONS

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a Certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in Section 8.1.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of the CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

Authorization Domain Name: The FQDN used to obtain authorization for Certificate issuance for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "*." from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.

Authorized Ports: One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first Domain Name node left of a registry controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

Baseline Requirements: The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates as published by the CA/Browser Forum and any amendments to such document.

CAA: From RFC 8659 (http:tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue Certificates for that domain name. CAA Resource Records allow a public Certification Authority to implement additional controls to reduce the risk of unintended Certificate mis-issue."

CA Key Pair: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Management System: A system used by a CA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. a Section in a CA's CPS or a certificate template file used by CA software.

Certificate Systems: The system used by a CA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.

Certificate Transparency: To ensure Certificates function properly throughout their lifecycle, TunTrust will log SSL Certificates with a public Certificate transparency database if the subscriber signs the subscriber agreement and therefore opts for the publication of the log containing information relating to his certificate. Because this will become a requirement for Certificate functionality, Subscriber cannot opt out of this process. Log server information is publicly accessible. Once submitted, information cannot be removed from a log server.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

Cross Certificate: A Certificate that is used to establish a trust relationship between two Root CAs.

CSPRNG: A random number generator intended for use in cryptographic system.

Delegated Third Party: A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits, but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Delegated Third Party System: Any part of a Certificate System used by a Delegated Third Party while performing the functions delegated to it by the CA.

DNS CAA Email Contact: The email address defined in Section A.1.1 of the Baseline Requirements.

DNS CAA Phone Contact: The phone number defined in section A.1.2 of the Baseline Requirements.

DNS TXT Record Email Contact: The email address defined in Section A.2.1 of the Baseline Requirements.

DNS TXT Record Phone Contact: The phone number defined in Section A.2.2 of the Baseline Requirements.

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Label: From RFC 8499 (<http://tools.ietf.org/html/rfc8499>): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."

Domain Name: An ordered list of one or more Domain Labels assigned to a node in the Domain Name System. Domain Namespace: The set of all possible Domain Names those are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Fully-Qualified Domain Name: A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.

Government Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation). In the context of Business Entities, the government agency in the jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected Certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

Individual: A natural person.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of Certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

IP Address: A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.

IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

Key Pair: The Private Key and its associated Public Key.

LDH Label: From RFC 5890 (<http://tools.ietf.org/html/rfc5890>): "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets."

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Multi-Factor Authentication: An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction: something you know (knowledge factor), something you have (possession factor), and something you are (inherence factor). Each factor must be independent. Certificate based authentication can be used as part of Multifactor Authentication only if the private key is stored in a Secure Key Storage Device.

Non-Reserved LDH Label: From RFC 5890 (<http://tools.ietf.org/html/rfc5890>): "The set of valid LDH labels that do not have '--' in the third and fourth positions."

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Parent Company: A company that Controls a Subsidiary Company.

P-Label: A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2 of the CA/B Forum Baseline Requirements.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the Certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate. Relying Parties must read and agree to TunTrust's relying party agreement available at https://www.tuntrust.tn/repository.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Request Token: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.

The Request Token SHALL incorporate the key used in the certificate request.

A Request Token MAY include a timestamp to indicate when it was created.

A Request Token MAY include other information to ensure its uniqueness.

A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.

A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.

A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation.

The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Note: Examples of Request Tokens include, but are not limited to:

 (i) a hash of the public key; or

 (ii) a hash of the Subject Public Key Info [X.509]; or

 (iii) a hash of a PKCS#10 CSR.

A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests.

Note: This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR.

```
echo `date -u +%Y%m%d%H%M` `sha256sum <r2.csr`\| sed "s/[ -]//g"
```

The script outputs:

201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

Requirements: The Baseline Requirements of the CA/B Forum.

Reserved IP Address: An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries:

https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root CA System: A system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Root Key Generation Script: A documented plan of procedures to be performed for the generation of the Root CA Key Pair.

Secure Key Storage Device: A device certified as meeting at least FIPS 140-2 level 2 overall, level 3 physical, or Common Criteria (EAL 4+)

Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties available at https://www.tuntrust.tn/repository.

Subsidiary Company: A company that is controlled by a Parent Company.

Technically Constrained Subordinate CA Certificate: A Subordinate CA Certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Test Certificate: This is no longer used in the CA/B Forum Baseline Requirements.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialist: Someone who performs the information verification duties specified by these Requirements.

Validity Period: Prior to 2020-09-01, the period of time measured from the date when the Certificate is issued until the Expiry Date. For Certificates issued on or after 2020-09-01, the validity period is as defined within RFC 5280, Section 4.1.2.5: the period of time from notBefore through notAfter, inclusive.

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

Wildcard Certificate: A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names contained in the Certificate.

Wildcard Domain Name: A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

XN-Label: From RFC 5890 (http://tools.ietf.org/html/rfc5890): "The class of labels that begin with the prefix"xn--" (case independent), but otherwise conform to the rules for LDH labels."

1.6.2 ACRONYMS

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CNI	Centre National Informatique
CP	Certificate Policy
CPS	Certification Practice Statement
CRA	Central Registration Authority
CRAO	Central Registration Authority Officer
CRL	Certificate Revocation List
CSP	Certification Service Provider
DBA	Doing Business As
DNS	Domain Name System

DRA   Delegated Registration Authority

ERA   Enterprise Registration Authority

FIPS   (US Government) Federal Information Processing Standard

FQDN   Fully-Qualified Domain Name

IANA   Internet Assigned Numbers Authority

ICANN   Internet Corporation for Assigned Names and Numbers

ISO   International Organization for Standardization

LRA   Local Registration Authority

NIST   (US Government) National Institute of Standards and Technology

OCSP   Online Certificate Status Protocol

OID   Object Identifier

PKI   Public Key Infrastructure

PVP   Physical Verification Point

PVPO   Physical Verification Point Officer

RA   Registration Authority

S/MIME   Secure MIME (Multipurpose Internet Mail Extensions)

SSL   Secure Sockets Layer

TLD   Top-Level Domain

TLS   Transport Layer Security VOIP Voice Over Internet Protocol

TN   Tunisia

TSP   Trust Service Provider

VoIP   Voice Over Internet Protocol

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

TunTrust makes the following available on its public repository at https://www.tuntrust.tn/repository:

- TunTrust CP/CPS;
- Subscriber contractual agreements (example: Subscriber Agreement, Application Forms, etc.);
- Audit Reports by Qualified Auditors;
- Certification Authority Certificates and related Authority Revocation Lists (ARLs);
- Certificate Revocation Lists (CRLs).

For further details regarding the publication of information refer to Section 2.2.

TunTrust ensures that revocation data for issued Certificates and its Root Certificates are available in accordance with the CP/CPS.

TunTrust applies best endeavors to ensure that the repository is not unavailable for longer than a maximum period of time of five (05) days per year (i.e. a total of no more than 05 overall days unplanned downtime per year).

2.2 Publication of Certification Information

TunTrust conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

TunTrust publishes information mentioned in Section 2.1 on its publicly accessible website https://www.tuntrust.tn/repository that is available on a 24x7 basis.

2.3 Time or Frequency of Publication

TunTrust reviews its CP/CPS at least annually and makes appropriate changes so that TunTrust CA operation remains accurate, transparent and complies with requirements listed in Section 8 of this document. TunTrust CA closely monitors CA/Browser Forum ballots and updates to the Baseline Requirements and implements updates to TunTrust operations in a timely manner.

Revision Table in Section 1.2 indicates reviews and updates made to this CP/CPS by adding a dated changelog entry and incrementing the CP/CPS version number, even if no other changes are made to the document.

New or modified versions of this CP/CPS, Subscriber Agreements, or Relying Party agreements are published within seven days after approval.

Publication frequency of CRLs and frequency of updating OCSP records are specified in Sections 4.9.7 and 4.9.9.

2.4 Access controls on repositories

Read-only access to Repositories is available. Logical and physical controls prevent unauthorized write access to repositories.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 TYPES OF NAMES

The Subscriber is described in the Certificate by a Distinguished Name pursuant to the X.501 standard. The description of the DN field contained in the Certificates is available in Annex B.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

TunTrust uses distinguished names (DN) that identify the Subscriber.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

TunTrust does not issue anonymous or pseudonymous Certificates.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

Fields contained in TunTrust Certificates are in compliance with this CP/CPS. In general, the rules for interpreting name forms can be found in International Telecommunication (ITU) and Internet Engineering Task Force (IETF) Standards, such as the ITU-T X.500 series of standards and applicable IETF RFCs.

3.1.5 UNIQUENESS OF NAMES

The full combination of the Subject Attributes (Distinguished Name) is unique within the boundaries defined by this CP/CPS and conforms to all applicable X.500 standards for the uniqueness of names.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

Not applicable. TunTrust does not issue certificates including trademarks.

3.2 Initial Identity Validation

TunTrust may perform identification of the Applicant using any legal means of communication or investigation necessary to identify the Legal Entity or individual.

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

Private Keys are generated and stored under the control of the Subscriber on a Hardware Security Module (HSM) that is located in TunTrust data center. Access by the Subscriber to the keys is protected using multifactor authentication.

3.2.2 AUTHENTICATION OF ORGANIZATION AND DOMAIN IDENTITY

TunTrust verifies the identity of the Applicant, and the authenticity of the Applicant's certificate request using a verification process meeting the requirements of Section 3.2.2.1.

3.2.2.1 IDENTITY

The verification of the identity of Applicants is performed by DRA using APIs provided by national registry database.

3.2.2.2 DBA/TRADENAME

Not applicable. TunTrust does not issue certificates including trademarks or DBA.

3.2.2.3 VERIFICATION OF COUNTRY

TunTrust verifies the country associated with the Subject using APIs provided by national registry database.

3.2.2.4 VALIDATION OF DOMAIN AUTHORIZATION OR CONTROL

Not applicable. TunTrust does not issue SSL certificates from this hierarchy of CAs.

3.2.2.5 AUTHENTICATION FOR AN IP ADDRESS

Not applicable. TunTrust does not issue certificates with IP addresses.

3.2.2.6 WILDCARD DOMAIN VALIDATION

Not applicable. TunTrust does not issue SSL certificates from this hierarchy of CAs.

3.2.2.7 DATA SOURCE ACCURACY

DRA uses Tunisian governmental entities as data sources and third party databases sourced from Tunisian governmental entities and regularly updated such that TunTrust considers it a reliable data source.

Before relying on any data provided, TunTrust will verify the following attributes:

a) The age of the information provided,
b) The frequency of updates to the information source,
c) The data provider and purpose of the data collection,
d) The public accessibility of the data availability, and
e) The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA RECORDS

Not applicable. TunTrust does not issue SSL certificates from this hierarchy of CAs.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

TunTrust implements rigorous authentication requirements to ensure that the identity of the Applicant is proven. This includes thorough identity validation at certificate application.

An identity validation of an individual Subscriber for issuance of a certificate, includes the following:

– The Subscriber must be physically present in front of a PVPO at certificate application.

– The Subscriber must provide for verification a valid and authentic ID photo (including national identity card, passport or residence permit).

The identify validation is also performed by the digital signature of the certificate request by the applicant using a valid certificate.

3.2.3.1 VALIDATION OF SUBSCRIBER EMAIL

Not applicable. Subscriber email is not included in the end user certificate.

3.2.3.2 VALIDATION OF SUBSCRIBER PHONE NUMBER

TunTrust takes reasonable measures to verify that the Applicant submitting the request controls the mobile phone number referenced in the Application form. The mobile phone number is not included in the certificate; however, it is used as a second authentication factor in a 2FA process required to activate the Subscriber private keys stored on the remote QSCD.

The mobile phone control is performed through a challenge-response procedure by sending a SMS OTP to the mobile phone number. The Applicant must respond with the received OTP within a limited time to demonstrate control over that phone number. DRA also verify that the applicant has control over the mobile phone number by requesting a APIs provided by telecom operators.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Unverified information is never included in TunTrust end entities Certificates. All Subscriber information included in Certificates are duly verified.

3.2.5 VALIDATION OF AUTHORITY

A face-to-face identification through physical presence is mandatory to validate the personal credentials of the Applicant by the PVP. The identification is also performed by the digital signature of the certificate request by the applicant using a valid certificate.

For Mobile-ID Certificates, the verification that the Applicant has control over the mobile phone number used to activate the Applicant private keys stored in the remote QSCD is detailed in Section 3.2.3.2.

3.2.6 CRITERIA FOR INTEROPERATION

Not applicable. TunTrust does not have any cross-certificates with other CAs.

3.3 Identification and authentication for re-key requests

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

Not Applicable. TunTrust does not support rekey.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

Not Applicable. TunTrust does not support rekey.

3.4 Identification and authentication for revocation request

Revocation requests are authenticated to ensure they emanate from authorized persons. The process how the revocation request can be submitted is described in Section 4.9.3.

TunTrust may also perform revocation on behalf of Subscribers in accordance with the requirements of the applicable Subscriber Agreement.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

TunTrust CA does not issue certificates to entities that reside in countries where the laws of TunTrust office location prohibit doing business. Unless specified by TunTrust applicable standards or the applicable CP/CPS, applications for end-entity certificates can be submitted by anyone who complies with provisions set within the registration forms and processes, the CP/CPS and the TunTrust end-user terms and conditions. TunTrust issues or revokes certificates only at authenticated request of the DRA.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

For provision of services, TunTrust operates a Central Registration Authority connected to a DRA under appropriate contracting agreements. Towards any party, TunTrust assumes full responsibility and accountability for acts or omissions of all third parties it uses to deliver certification services.

The Applicant commits to providing a current, genuine and complete certificate request and all evidence requested by TunTrust.

TunTrust guarantees that all required verifications have been performed prior to successful registration leading to certificate issuance and that all certificate requests submitted to the Issuing CA are complete, accurate, valid and duly authorized. It also guarantees the accuracy of all information contained in the Certificate.

Face-to-face identification is performed through a face-to-face identification provided by a PVP.

4.2 Certificate Application Processing

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

TunTrust does not re-use previous validation information. Each certificate application must go through all validation functions described in Section 3.2.

- Applicant must register on the website https://www.mobile-id.tn and fill in the online order form.

- Application must include the following items:

  o Given name and surname of the applicant,

  o Birth date,

  o Number of the national identity card,

  o Phone number,

- The following verification tasks are performed by the DRA:

  o Order Form is duly filled,

  o Applicant has been informed of and accepted the Subscriber Agreement and Terms of Use of the Certificate,

  o Verification of both the national identity card number and the Mobile Phone Number through APIs provided by the telecom operators in order to make sure that the mobile phone number provided was registered with the national identity card number that was provided in the

Application form,

- o Control of the Mobile Phone Number is verified through APIs by a challenge response mechanism.

  Note: The Mobile ID Application will be processed after the challenge-response verification of the mobile phone number is deemed successful,

- o Verification of the link between the given name and surname and the provided identity card number in the national registry database.

Upon the successful verification of the Certificate Application and the face-to-face identification of Applicant by a PVP or the digital signature of the certificate request signed by the Applicant using a valid Certificate, the CRA initiates a certificate signing request using multi-factor authentication.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

TunTrust will approve or reject an Applicant's Certificate request based upon the Applicant meeting the requirements of this CP/CPS and all applicable laws and regulations.

TunTrust rejects any certificate application that TunTrust cannot verify.

TunTrust, in its sole discretion, may refuse to accept an application for a Certificate, and may refuse to issue a Certificate, without incurring any liability for loss or damages arising out of such refusal. TunTrust reserves the right not to disclose reasons for such a refusal. Applicants whose applications have been rejected may subsequently re-apply.

TunTrust, at its sole discretion not to be unreasonably withheld, may override any decision to approve Applicant's Certificate request.

TunTrust CAs do not issue certificates containing Internal Names or Reserved IP Addresses (see Section7.1.4.2).

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

Under normal circumstances, TunTrust confirms Certificate application information and issues a Certificate within seven working days as established by Tunisian national law.

4.3 Certificate Issuance

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

TunTrust CRA proceeds to the following:

- Verify the source of the certificate request,
- Create private key of subscriber in the QSCD,
- Issue a Certificate signing request,
- Send the CSR to the concerned issuing CA.

Following successful completion of the registration process, Issuing CA proceeds to the Certificate issuance process.

Databases and CA processes occurring during certificate issuance are protected from unauthorized modification.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The Applicant will be notified that the Certificate is issued via the phone number that were supplied by the Subscriber during the enrollment process.

The subscriber receive the PIN code of the private key activation by the same phone number.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

A Subscriber that accepts a Certificate warrants to TunTrust, that all information supplied in connection with the application process and all information included in the Certificate issued to them is true, complete, and not misleading. Without limitation to the generality of the foregoing, the use of a Certificate signifies acceptance by that Subscriber of this CP/CPS and Subscriber Agreement (as the same may, from time to time, be amended or supplemented) by which they irrevocably agree to be bound.

If the subscriber is not satisfied with the details contained within the Certificate, he or she must email assistance@tuntrust.tn explaining why the certificate is not being accepted. This communication must take place within 30 days of issuance. Certificates are considered accepted 30 days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.4.2 Publication of the certificate by the CA

Refer to Section2.1.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers have to protect their Private Key to avoid disclosure to third parties. TunTrust provides a Subscriber Agreement which highlights the obligations of the Subscriber with respect to Private Key protection.

Subscribers are bound to use the Certificate for its lawful and intended purposes only.

4.5.2 Relying Party Public Key and Certificate Usage

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

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

Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

- – The appropriateness of the use of the Certificate for any given purpose and that the use is not prohibited by this CP/CPS.

- That the Certificate is being used in accordance with its Key-Usage field extensions.
- That the Certificate is valid at the time of reliance by reference to Online Certificate Status Protocol or Certificate Revocation List checks.

4.6 Certificate renewal

Certificate Renewal means the issuance of a new Certificate without changing the Public Key or any other information in the Certificate. Certificate renewal is not supported by TunTrust.

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.2 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.3 WHO MAY REQUEST RENEWAL

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.4 PROCESSING CERTIFICATE RENEWAL REQUESTS

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.5 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.6 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.7 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.8 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable. Certificate renewal is not supported by TunTrust.

4.7 Certificate Re-Key

Certificate re-key means the issuance of a new certificate with a new public key, but the same subject identity information.

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

4.7.1.1 RE-KEY OF DEVICE CERTIFICATES

Not Applicable. TunTrust does not re-key device certificates.

4.7.1.2 RE-KEY OF END-USER CERTIFICATE

Issuing CA may re-key certificates provided that the following conditions are met:

- The applicant must sign the application request with a valid certificate;
- All details of the certificate remain accurate and no new validation of identity is required.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

In accordance with the conditions specified in previous section, Certificate re-key may be requested by an DRA and the subscriber for his own individual certificate.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUEST

Only after verifying re-key request from subscriber or DRA processing of certificate re-keying request shall be initiated.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Notification of issuance of a re-keyed certificate by the Issuing CA to Subscribers shall follow the same procedures as notification for newly issued certificates.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Conduct constituting acceptance of a re-keyed certificate is same as listed in section 4.4.1.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

After successful completion of the re-key process, the certificate shall be published in appropriate repositories, in the same manner as for a newly issued certificate.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Generally, TunTrust CAs do not notify other entities of a re-keyed certificate.

4.8 Certificate Modification

Certificate modification is the process through which a Subscriber requests a Certificate with modified subject information. TunTrust considers such request as an initial registration request. The requester is therefore required to start a new Certificate request.

4.8.1 CIRCUMSTANCES FOR CERTIFICATE MODIFICATION

Not Applicable. TunTrust does not support Certificate modification.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

Not Applicable. TunTrust does not support Certificate modification.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

Not Applicable. TunTrust does not support Certificate modification.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable. TunTrust does not support Certificate modification.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

Not Applicable. TunTrust does not support Certificate modification.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

Not Applicable. TunTrust does not support Certificate modification.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable. TunTrust does not support Certificate modification.

4.9 Certificate Revocation and suspension

4.9.1   CIRCUMSTANCES OF REVOCATION

Certificate revocation is the process by which TunTrust prematurely terminates the Validity Period of a Certificate. TunTrust will make its certificate revocations public through the use of publicly issued CRLs and publicly available OCSP responder services.

4.9.1.1   REASONS FOR REVOKING A SUBSCRIBER CERTIFICATE

TunTrust revokes a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that TunTrust revokes the Certificate;
2. The Subscriber notifies TunTrust that the original Certificate request was not authorized and does not retroactively grant authorization;
3. TunTrust obtains a request of revocation from the DRA;
4. TunTrust obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
5. TunTrust is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); or

TunTrust revokes a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. TunTrust obtains evidence that the Certificate has been used for a purpose outside of that indicated in the Certificate or in TunTrust's Subscriber Agreement;
3. TunTrust receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
4. TunTrust receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
5. TunTrust is made aware that the Certificate was not issued in accordance with this Certificate Policy / Certification Practice Statement;
6. TunTrust determines or is made aware that any of the information appearing in the Certificate is inaccurate;
7. TunTrust ceases operations for any reason and has not arranged for another CA to provide revocation support for the certificate; or
8. TunTrust CA private key used in issuing the certificate is suspected to have been compromised.

4.9.1.2   REASONS FOR REVOKING A SUBORDINATE CA CERTIFICATE

TunTrust will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

a) The Subordinate CA requests revocation in writing;
b) The Subordinate CA notifies TunTrust that the original certificate request was not authorized and does not retroactively grant authorization;

c) TunTrust obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and6.1.6,

d) TunTrust obtains evidence that the Certificate was misused;

e) TunTrust is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the applicable CP/CPS;

f) TunTrust determines that any of the information appearing in the Certificate is inaccurate or misleading;

g) TunTrust or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

h) TunTrust or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless TunTrust has made arrangements to continue maintaining the CRL/OCSP Repository; or

i) Revocation is required by TunTrust CP/CPS.

4.9.2 WHO CAN REQUEST REVOCATION

TunTrust accepts authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or through the DRA.

Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports to notify TunTrust of a suspected reasonable cause to revoke the Certificate. Problem Reports shall be submitted to the Contact Person specified in Section1.5.2. TunTrust may also at its own discretion revoke Certificates.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

A revocation request should be promptly and directly communicated to TunTrust. A revocation request may be submitted using one of the following methods:

− The Subscriber may revoke his/her Certificate by logging in to his/her personal space at https://www.mobile-id.tn.

− For Certificate Problem Report submitted by third parties to the Contact Person specified in Section 1.5.2, TunTrust personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
   o The nature of the alleged problem,
   o The evidence provided in support of the request,
   o The urgency of the request,
   o The number of reports received about a particular certificate or website,
   o The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
   o Tunisian National Legislation.

4.9.4 REVOCATION REQUEST GRACE PERIOD

No grace period is permitted once a revocation request has been verified. TunTrust will revoke Certificates according to Section 4.9.1.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

Within 24 hours after receiving a Certificate Problem Report, TunTrust will investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, TunTrust will work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which TunTrust will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation does not exceed the time frame set forth in Section4.9.1.1.

4.9.6 REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

Relying parties must validate every Certificate against the most updated CRL as minimum. Alternatively, relying parties may check Certificate status using OCSP.

4.9.7 CRL ISSUANCE FREQUENCY

For the status of TunTrust CAs certificates:

- TunTrust updates and reissues CRLs at least (i) once every twelve months and (ii) within 24 hours upon revoking a Subordinate CA Certificate, and the value of the nextUpdate field is not more than twelve months beyond the value of thisUpdate field.

For the status of Subscriber Certificates:

- The CRL of the issuing CAs are issued every twenty-four (24) hours or whenever a certificate is revoked. The value of the nextUpdate field must not be more than six days beyond the value of thisUpdate field. The OCSP responder will report a certificate revoked immediately after the revocation has been completed.

4.9.8 MAXIMUM LATENCY FOR CRLs

The CRLs of TunTrust CA are issued according to Section 4.9.7 and published in a timely manner. The revocation shall become effective immediately upon its publication.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

TunTrust supports OCSP responses in addition to CRLs. Response times are generally no longer than 05 seconds under normal network operating conditions.

TunTrust OCSP responses conforms to RFC 6960 and/or RFC 5019. OCSP responses are signed by an OCSP Responder whose Certificate is signed by TunTrust CA that issued the Certificate whose revocation status is being checked. OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

The OCSP responder operated by TunTrust supports the HTTP GET method as described in RFC 6960 and/or RFC 5019.
The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

Relying Parties must confirm revocation information otherwise all warranties become void.

- For the status of Subscriber Certificates: TunTrust OCSP responses have a validity interval greater than or equal to eight hours;
- TunTrust OCSP responses have a validity interval less than or equal to ten days;
- TunTrust OCSP responses have validity intervals less than sixteen hours, therefore TunTrust updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.

- For the status of Subordinate and Issuing CA Certificate:

- TunTrust updates information provided via an OCSP at least (i) every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP Responder receives a request for the status of a Certificate serial number that is "unused", then the responder do not respond with a "good" status.

A certificate serial number within an OCSP request is one of the following three options:

1. "assigned" if a Certificate with that serial number has been issued by MOBILE ID ISSUER CA, using any current or previous key associated with that CA subject; or

2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by (a) MOBILE ID ISSUER CA; or (b) a Precertificate Signing Certificate [RFC6962] associated with MOBILE ID ISSUER CA; or

3. "unused" if neither of the previous conditions are met.

TunTrust requires OCSP requests to contain the following data:

- Protocol version,
- Service request,
- Target Certificate identifier.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

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

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

Should a Private Key become compromised, the related Certificate shall immediately be revoked. Should the private CA key become compromised, all Certificates issued by that CA shall be revoked.

In order to demonstrate Key Compromise, Parties must submit Certificate problem reports to TunTrust (refer to Section 1.5.2) that include one of the following methods:

- Providing the Private Key itself,
- Providing references to vulnerability and/or security incident sources from which the Key Compromise is verifiable.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

No suspension of Certificates is performed by TunTrust.

4.9.14 WHO CAN REQUEST SUSPENSION

No suspension of Certificates is performed by TunTrust.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

No suspension of Certificates is performed by TunTrust.

4.9.16 LIMITS ON SUSPENSION PERIOD

No suspension of Certificates is performed by TunTrust.

4.10 Certificate Status Services

4.10.1 OPERATIONAL CHARACTERISTICS

TunTrust provides a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both in the certificates. TunTrust does not remove revocation entries on CRL or OCSP until after the Expiry Date of the revoked Certificate.

4.10.2 SERVICE AVAILABILITY

TunTrust operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of five (05) seconds or less under normal operating conditions.

TunTrust maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by TunTrust.

TunTrust provides a globally available OCSP and CRL service availability at all times, with outages constrained to be within the limits expressed in Section2.1.

TunTrust maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 OPERATIONAL FEATURES

The OCSP Responder is available for all types of certificates issued by TunTrust.

4.11 End of Subscription

Subscribers may end their subscription to Certificate services by having their Certificate revoked or naturally letting it expire.

4.12 Key Escrow and recovery

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

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

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

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

TunTrust does not provide session key encapsulation and recovery.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

TunTrust develops, implements, and maintains a comprehensive information security policy designed to:

a) Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;

b) Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;

c) Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;

d) Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and

e) Comply with all other security requirements applicable to TunTrust by law.

The Certificate Management Process includes:

a) physical security and environmental controls;

b) system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;

c) network security and firewall management, including port restrictions and IP address filtering;

d) user management, separate trusted-role assignments, education, awareness, and training; and

e) logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

TunTrust performs an annual Risk Assessment that:

a) Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

b) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and

c) Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that TunTrust has in place to counter such threats.

Based on the Risk Assessment, TunTrust develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes.

The security plan also considers then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical controls

5.1.1 SITE LOCATION AND CONSTRUCTION

TunTrust CA's primary and secondary data centers are in Tunis, Tunisia. TunTrust data center exhibits the following features:

- Protected by physical barriers, including solid walls that extend from real floor to real ceiling to prevent unauthorized entry and environmental contamination to the CAs certificate manufacturing facility,
- Not located in areas likely to exhibit hazard of environmental damage, chemical, biological or radiological pollution,
- Physically separated areas for visitor reception, clearance and computer equipment hosting,
- Capable of safely storing, separate to any computer equipment, fuel to power facilities in the event of loss of mains power.

5.1.2 PHYSICAL ACCESS

Entry to TunTrust Data Centers containing the CAs certificate manufacturing facility is achieved only through a limited number of access points controlled by security personnel on duty full time (24 hours per day, 365 days per year).

Intruder detection systems including infrared walls are installed and regularly tested to cover all external doors of the data centers housing the CA operational facilities.

All critical CA operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software. Such systems are physically separated from the organization's other systems so that only authorized employees of the CA can access them. The secure parts of TunTrust CA hosting facilities are protected using physical access controls with biometric scanners or card access systems making them accessible only to appropriately authorized individuals. CA operational facilities are physically locked and alarmed when unoccupied.

All personnel and visitors entering and leaving CA operational facilities are logged. Entry, exit, and activities within CA facilities are under constant video surveillance. Third party support services personnel are granted restricted access to secure CA operational facilities only when required and such access is authorized and accompanied. Access rights to CA facilities are regularly reviewed and updated.

5.1.3 POWER AND AIR CONDITIONING

TunTrust CA operates within data centers that have primary and secondary power supplies to ensure continuous, uninterrupted access to electric power. Redundant backup power is provided by battery uninterrupted power supplies (UPS) and one generator.

TunTrust data centers are equipped with heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 WATER EXPOSURES

No data center is in a known flood risk area. All TunTrust CAs certificate manufacturing facility have sealed roofs to prevent water exposure.

HVAC systems are in place to prevent humidity buildup. All data centers have policies preventing the taking of liquids (e.g. drinks) into the cabinet areas.

5.1.5 FIRE PREVENTION AND PROTECTION

TunTrust has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke.

Fire doors exist on security perimeters around CA operational facilities and are alarmed.

TunTrust's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 MEDIA STORAGE

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

5.1.7 WASTE DISPOSAL

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

5.1.8 OFF-SITE BACKUP

TunTrust maintains copies of CA private keys, archived audit logs, and other sensitive information at secured offsite locations. All copies of TunTrust CA private keys are stored in a system or device validated as meeting FIPS 140 Level 3 to ensure that they are only accessible by trusted personnel.

5.2 Procedural Controls

5.2.1 TRUSTED ROLES

The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of TunTrust. All personnel appointed to a trusted role had a background check prior to allowing such person to act in a trusted role. A list of personnel appointed to trusted roles is maintained and reviewed at least annually.

The following roles are deemed to be trusted roles:

Validation Specialist	They are responsible for routine certification services such as customer services and revocation. A person to whom this role is assigned can be a shareholder of CA private keys activation data.
System Administrator	The System Administrator is responsible for the installation and configuration of PKI components (CA, RA, VA, ...). This administrator is also responsible for keeping PKI systems updated with software patches and other maintenance needed for system stability and recoverability.

	A person to whom this role is assigned can be a shareholder of CA private keys activation data.
System Operator	The System Operator is responsible for the installation and configuration of the system hardware, including servers and different components of the Front End / Internal Support System. The System Administrator is also responsible for keeping systems updated with software patches and other maintenance needed for system stability and recoverability. A person to whom this role is assigned can be a shareholder of CA private keys activation data.
Application Administrator	The Application Administrator is responsible for the installation, configuration and operations of the applications related to TunTrust.
Physical and Logical Security Officer	The Physical and Logical Security Officer is responsible for the installation and configuration of the physical security platforms (access control, video surveillance, IDS, ...) and the logical security platforms (firewalls, WAF, routers, network configuration). A person to whom this role is assigned can be a shareholder of CA private keys activation data.
Auditor	The Auditor is authorized to view archives and audit logs. The auditor is also responsible for overseeing internal compliance to determine if TunTrust is operating in accordance with this CP/CPS. This includes acting as internal auditor in TunTrust key ceremonies. A person to whom this role is assigned cannot be a shareholder of CA private keys activation data.
Key/Ceremony Manager	The Key/Ceremony Manager is responsible of conducting the key ceremonies.
Shareholders	Holders of secret shares needed to operate TunTrust CA private keys.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

Handling of CA Private Keys (throughout the entire CA key lifecycle) requires the involvement of at least two trusted persons. Physical and logical access controls exist for the key activation material in order to maintain multi-party and multifactor control over the Hardware Security Modules containing CA Private Keys.

Shareholders use HSM Smartcards for authentication. The HSM itself enforces dual control based on the HSM smartcards for the different functions. The number of needed HSM-smartcards (m) of the total number of produced HSM-smartcards (n) is:

(a) Key generation = 3 of 6

(b) Signing key activation = 2 of 6

(c) Private key backup and restore = 3 of 6

5.2.3   IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

All personnel are required to authenticate themselves before they are allowed access to systems necessary to perform their trusted roles.

5.2.4   ROLES REQUIRING SEPARATION OF DUTIES

No person can have more than one of the roles listed in Section 5.2.1 at a time.

To accomplish this separation of duties, TunTrust specifically designates individuals to trusted roles. TunTrust's systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3 Personnel controls

5.3.1   QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS
TunTrust must abide by Tunisian public sector recruitment procedures based on open competition assessing the Qualifications, Experience, Clearance and Training of the candidates as appropriate to the job function.

Prior to the engagement of TunTrust employee in the Certificate Management Process, TunTrust verifies the identity and trustworthiness of such person who must be a TunTrust permanent employee. All TunTrust personnel must sign the internal security charter. Trusted roles and responsibilities, as specified in Section 5.2.1 are documented in job descriptions. TunTrust personnel have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

5.3.2   BACKGROUND CHECK PROCEDURES

All TunTrust personnel are subject to Tunisian public sector recruitment and selection procedures prior to employment. These procedures undergo background checks, to the extend allowable by law, including, at a minimum:

- – criminal records checks,
- – employment and education history,
- – identity checks using government issued photo ID.

Personnel do not have access to the trusted functions until any necessary checks are completed and results analyzed. All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and are subject to background investigation at least every five years.

5.3.3   TRAINING REQUIREMENTS
TunTrust provides suitable training to all staff before they take on a Trusted Role should they not already have the complete skill-set required for that role. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.
TunTrust provides all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including this CP/CPS), common threats to the information verification process (including phishing and social engineering), and the CA/B Forum requirements.

TunTrust maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

TunTrust documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

TunTrust requires all Validation Specialists to pass an examination provided by TunTrust on the information verification requirements outlined in this CP/CPS.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

All personnel in Trusted Role maintain skill levels consistent with TunTrust's training and performance programs.

Individuals responsible for trusted roles are aware of changes in TunTrust CA or RA operations, as applicable. Any significant change to the operations has a training) plan, and the execution of such plan is documented.

TunTrust provides an information security and privacy training at least once a year to all employees.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

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

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

All employees of TunTrust are made aware that performing actions outside the rules established by operational regulation, security policy or privacy policy carries the possibility of disciplinary action as per TunTrust internal rules and Tunisian Public sector disciplinary procedures.

Should that violation of company policy encompass potential criminal wrongdoing, TunTrust will report the matter to the appropriate law enforcement bodies for further investigation and action as stated in the Tunisian Public sector disciplinary procedures.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

TunTrust does not assign Trusted Roles to external Contractors.

All contract arrangements between contractors and TunTrust for the provision of temporary contract personnel allow TunTrust to take measures against contract staff who violate TunTrust security policies.

Protective measures may include (i) bonding requirements on contract personnel; (ii) indemnification for damages due to contract personnel willful harmful actions; and (iii) financial penalties.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

Personnel are granted access to relevant training documents and governance documents as their intended roles dictate. Other technical, operational and administrative documents (e.g., administrator manuals, user manuals, etc.) are provided in order for the trusted personnel to perform their duties.

5.4 Audit Logging Procedures

5.4.1 TYPES OF EVENTS RECORDED

TunTrust and the DRA record events related to the security of its Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems. TunTrust records events related to their actions taken to process a Certificate request and to issue a Certificate, including all information generated and documentation received in connection with the Certificate request; the time and date; and the personnel

involved. TunTrust makes these records available to its Qualified Auditor. TunTrust records at least the following events:

1. CA Certificate and key lifecycle events, including:

    1. Key generation, backup, storage, recovery, archival, and destruction;

    2. Certificate requests, renewal, and re-key requests, and revocation;

    3. Approval and rejection of certificate requests;

    4. Cryptographic device lifecycle management events;

    5. Generation of Certificate Revocation Lists;

    6. Signing of OCSP Responses (as described in Section 4.10); and

    7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

2. Subscriber Certificate lifecycle management events, including:

    1. Certificate requests and revocation;

    2. All verification activities stipulated in the Baseline Requirements and this CP/CPS;

    3. Approval and rejection of Certificate requests;

    4. Issuance of Certificates;

    5. Generation of Certificate Revocation Lists; and

    6. Signing of OCSP entries Responses (as described in Section 4.10).

3. Security events, including:

    1. Successful and unsuccessful PKI system access attempts;

    2. PKI and security system actions performed;

    3. Security profile changes;

    4. Installation, update and removal of software on a Certificate System;

    5. System crashes, hardware failures, and other anomalies;

    6. Firewall and router activities; and

    7. Entries to and exits from the CA facility.

Log records include the following elements:

    1. Date and time of event;

    2. Identity of entity and/or operator that caused the record; and

    3. Description of the event.

All TunTrust CA components are regularly synchronized with a reliable time service. TunTrust CA uses a GPS-NTP time source to establish the correct time for accurate recording of automated log events.

Private keys in any form (e.g. plaintext or enciphered) are never recorded in Audit Logs.

5.4.2 FREQUENCY OF PROCESSING AUDIT LOG

The logging process allows real-time recording of transactions to identify abnormalities related to failed attempts (access or instruction). In case of manual input, writing is made the same business day as the event. Log events deemed to be security sensitive will automatically generate security incident reports that are handled as defined in Section 5.7.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

Section TunTrust retains for at least 20 years as per Tunisia national law:

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of:
    1. the destruction of the CA Private Key; or
    2. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the CA field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1(2)) after the expiration of the Subscriber Certificate;

Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

TunTrust makes these audit logs available to its Qualified Auditor upon request.

5.4.4 PROTECTION OF AUDIT LOG

Audit logs are stored within TunTrust primary location and in an off-site location. Access and security controls are in place to prevent alteration with the audit log. Production and archived logical audit logs are protected using a combination of physical and logical access controls.

All automated log events are recorded real-time to a secured central logging services in order to prevent log shrinkage or unexpected alteration. Logs stored offsite reside in facilities which have protections at least equivalent to the TunTrust originating systems.
Off-site logs are digitally signed to make tampering of the logs evident. The encryption key used for signing audit logs is not used for any other purpose. Offsite logs are verified periodically to ensure that their integrity has been maintained.

5.4.5 AUDIT LOG BACKUP PROCEDURES

For CA components that allow the configuration of multiple logging end-points, automated log events are recorded real-time to central logging services located at TunTrust Primary datacenter and at the secondary data center as an DR site location.

For CA components that do not support multiple logging end-points, TunTrust makes backup copies of audit logs on a monthly basis according to internal backup procedures. These copies are kept in a safe protected using physical access controls.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

Automated audit data is generated and recorded at the application, network and operating system level. All automated audit logs are sent to a central logging service for collation and review. Manually generated audit data is recorded by TunTrust personnel assigned to Trusted Roles.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

TunTrust is not required to notify a subject that it has been the cause of an auditable event.

5.4.8 VULNERABILITY ASSESSMENTS

TunTrust undergoes a vulnerability scan (i) within one (1) week of receiving a request from the CA/Browser Forum, (ii) after any system or network changes that TunTrust determines are significant, and (iii) at least every three (3) months on public and private IP addresses identified as TunTrust's Certificate Systems. TunTrust also undergoes a Penetration Test on Certificate Systems on at least an annual basis and after infrastructure or application upgrades that TunTrust determines are significant.

TunTrust records will be maintained in a manner reasonably sufficient to demonstrate that each Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.

TunTrust maintains and implements a formal documented vulnerability management process that includes identification, review, response, and remediation of vulnerabilities as described in Section 6.6.

Additionally, TunTrust performs annual risk assessments that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Process;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that TunTrust has in place to counter such threats.

5.5 Records archival

5.5.1 TYPES OF RECORDS ARCHIVED

TunTrust archives all audit logs (as set forth in Section 5.4.1).

Additionally, TunTrust archives:

1. Documentation related to the security of its Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems;

2. Documentation related to its verification, issuance, and revocation of certificate requests and Certificates.

TunTrust backs up application, network and system data including

- Registration information of Subscribers (signed subscriber agreements, IDs of Subscribers, signed Certificate request Forms, proof of legal existence of the organization, etc.),
- Configuration files of TunTrust CA systems,
- All audit logs listed in Section 5.4.1,

- Certificate lifecycle information.
- All versions of the CP/CPS and internal documents, including security policies and procedures,
- Ceremony scripts of TunTrust CA key events.

5.5.2 RETENTION PERIOD FOR ARCHIVE

Archived audit logs (as set forth in Section 5.5.1 are retained for a period of at least twenty (20) years from their record creation timestamp, or as long as they are required to be retained per Section5.4.3, whichever is longer.

Additionally, TunTrust retains, for at least twenty (20) years:

1. All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in Section 5.5.1); and
2. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of:
   1. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or
   2. the expiration of the Subscriber Certificates relying upon such records and documentation.

5.5.3 PROTECTION OF ARCHIVE

Physical and logical access controls are in place to prevent unauthorized access to archived data in electronic form. Archives are retained and protected against modification or destruction. Only specific TunTrust Trusted Roles, and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law.

5.5.4 ARCHIVE BACKUP PROCEDURES

TunTrust maintains and implements backup procedures so that in the event of the loss or destruction of the primary archives a complete set of backup copies is readily available.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

TunTrust ensures that the precise time of archiving all events, records and documents listed in Section 5.4 and 5.5 is recorded. This is accomplished through accurate NTP synchronization of all systems with TunTrust GPS-NTP time server. Records in paper format have a manually entered date and time.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

Archive information is collected internally by TunTrust.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVED INFORMATION

TunTrust will not divulge archive information to any external party except as follows:

- where a competent legal authority presents a warrant compelling the release of archived data; or
- where an audit requires archived data in order to complete a compliance report.
- where archived data is electronically generated, the signatures and encryption of this data are checked to ensure its integrity was maintained.

5.6 Key changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, TunTrust ceases using its expiring CA Private Key to sign Certificates (six years prior to its expiration) and uses the old Private Key only to sign CRLs until the expiry of the last certificate issued under it.

A new CA signing key pair is commissioned and all subsequently issued certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration. The corresponding new CA public key certificate is provided to Subscribers and relying parties through the delivery methods detailed in Section6.1.4.

5.7 Compromise and disaster recovery

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

TunTrust has an Incident Response Procedure and a Disaster Recovery Plan. TunTrust documents a business continuity procedure and disaster recovery plan designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure.

TunTrust does not disclose business continuity plans to Subscribers, Relying Parties, or to Application Software Suppliers, but will provide business continuity procedure and the risk treatment plan to TunTrust auditors upon request.

TunTrust annually tests, reviews, and updates these procedures. The business continuity procedure includes:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan,
6. Awareness and education requirements,
7. The responsibilities of the individuals,
8. Recovery time objective (RTO),
9. Regular testing of contingency plans,
10. TunTrust's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes,
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,
12. What constitutes an acceptable system outage and recovery time,
13. How frequently backup copies of essential business information and software are taken,
14. The distance of recovery facilities to TunTrust's main site, and
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

Every HSM in TunTrust primary site has a twin unit in the TunTrust disaster recovery site, maintained in standby, able to take over the role of the primary in the event of corruption. TunTrust follows its Disaster

Recovery Plan and Business Continuity Procedure in order to recover TunTrust CA operations, giving priority to the ability to generate Certificate status information and thereafter certificate revocation and issuance.

TunTrust CA hosts including Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are built and maintained by a consistent configuration management process. Configuration changes to these systems are automatically captured and sent to a central monitoring service to determine whether any changes violated the CA's security policies.

If TunTrust determines that such systems have been compromised, TunTrust will investigate the extent of the compromise and after ensuring the integrity of the CA systems, TunTrust will re-initiate its operations on replacement hardware located at the off-site facility, using back-up copies of its software, data, and Private Keys. TunTrust reserves the right to revoke affected Certificates and to provide new public keys to users.

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

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

a) Collect all information related to the incident (and if the event is ongoing, ensure that all data are being captured and recorded);

b) Begin investigating the incident and determine the degree and scope;

c) The Incident Response Team determines the course of action or strategy that should be taken (and in the case of Private Key compromise, determining the scope of Certificates that must be revoked);

d) Contact law enforcement, and other interested parties and activate any other appropriate additional security measures;

e) Monitor system, continue the investigation, ensure that all data is still being recorded as evidence and make a forensic copy of data collected;

f) Isolate, contain and stabilize the system, applying any possible short-term fixes needed to return the system to a normal operating state;

g) Prepare an incident report that analyzes the cause of the incident and implement a long-term solutions.

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

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

TunTrust Disaster Recovery Plan is tested, verified and updated at least annually to be operational in the event of a disaster.

TunTrust systems are redundantly configured at its primary facility and are mirrored at a separate geographically location for failover in the event of a disaster. TunTrust keeps activation data of the HSM of the disaster recovery site at a second separate geographically location.

If a disaster causes TunTrust PKI operations to become inoperative at the primary site, TunTrust will re-initiate its operations at its disaster recovery site, following the Disaster Recovery Plan and Business Continuity Procedure in order to recover TunTrust CA operations, giving priority to the ability to generate Certificate status information and thereafter certificate revocation and issuance.

5.8 CA or RA Termination

In case of termination of CA operations for any reason whatsoever, TunTrust will take the following steps prior to the termination:

Provide subscribers of valid certificates, the operators of the browser root certificate programs and the CA/B Forum with ninety (90) days' notice of its intention to cease acting as a CA,

- Revoke all certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking subscriber's consent,

- Destroy all private keys,

- Give timely notice of revocation to each affected Subscriber.

If a successor CA is found which can adopt all of TunTrust CA's responsibilities under its governing documentation, notification to the above shall also be provided explaining this succession. In such a case, the mass revocation may not be warranted.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 KEY PAIR GENERATION

6.1.1.1 CA KEY PAIR GENERATION

For the Mobile ID Root CA Key Pairs, TunTrust performs the following controls:
1. prepares and follows a Key Generation Script,
2. has a Qualified Auditor witness the Root CA Key Pair generation process or records a video of the entire Root CA Key Pair generation process, and
3. has a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

In all cases, TunTrust performs the following controls:
1. generates the CA Key Pair in a physically secured environment as described in Section 5.1 of this CP/CPS;
2. generates the CA Key Pair using personnel in trusted roles under the principles of multiple person control and split knowledge as disclosed in Section 6.2.1 of this CP/CPS;
3. generates the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in Section 6.2.2 of this CP/CPS;
4. logs its CA Key Pair generation activities and log all physical access during the key ceremony as disclosed in Section 5.4 ; and
5. maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in Section 6.2 of this CP/CPS and its Key Generation Script.

6.1.1.2 RA KEY PAIR GENERATION

No key pair generation is made for TunTrust RA.

6.1.1.3 SUBSCRIBER KEY PAIR GENERATION

For Subscriber keys generated by TunTrust, Key generation is performed in a secure cryptographic device that meets FIPS 140-2 level 3 using key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6.

For Qualified Certificates, Subscriber keys are generated and stored within a recognized Qualified Signature Creation Device (QSCD). The QSCD certification status is monitored and appropriate measures will be taken if the certification status of a QSCD changes.

Keys for certificates for the remote electronic signature are generated in an HSM that implements standards and control functions as specified in the Section 6.2.1 and kept in a secure environment for electronic signature creation.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

In the case of TunTrust physical QSCD end-user devices, the certificate:

- Is generated securely within the TunTrust QSCD, in accordance with the QSCD requirements,

- Has its corresponding Public Key certified by the CA.

Subscriber key pairs are generated on a remote QSCD by the CRA

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

The private keys are kept in a secure environment for electronic signature creation on behalf of the signatory. Subject of certification or Authorized Representative access the private key using two-factor authentication and private key activation PIN, when creating electronic signature.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

TunTrust publishes all CA certificates on its online repository https://www.tuntrust.tn/repository.

6.1.5 KEY SIZES

TunTrust Certificates meet the following requirements for algorithm type and key size:

6.1.5.1 ROOT CA CERTIFICATE:

	Value
Digest algorithm	SHA-512
ECDSA modulus size (bits)	512

6.1.5.2 SUBORDINATE CA CERTIFICATES

Issuing CA Certificates:

	Value
Digest algorithm	SHA-384
ECDSA modulus size (bits)	384

6.1.5.3 SUBSCRIBER CERTIFICATES:

	Value
Digest algorithm	SHA-256
ECDSA modulus size (bits)	256

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

TunTrust uses an HSM device that conforms to FIPS 186-2 and provides random number generation and onboard generation of up to 512 bit ECDSA Public Key.

TunTrust uses CA software that performs quality checks on generated keys for both RSA and ECC algorithms and also performs regular internal audits against randomly selected samples of Subscriber Certificates per Section8.7.

6.1.7 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

Private Keys corresponding to Root Certificates are not used to sign Certificates except in the following cases:
- Self-signed Certificates to represent the Root CA itself;
- Certificates for Subordinate CAs.

The key usage extension is set in accordance with the certificate profile requirements specified in Section7.1.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

TunTrust implements physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above consists of physical security and encryption, implemented in a manner that prevents disclosure of the CA Private Key. TunTrust encrypts its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

For subscriber keys, TunTrust requires that the private key holder uses reasonable steps to protect the key, such as restrictive permissions and possibly key encryption using a strong passphrase.

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

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

- Root CA keys: The HSM used for CA keys meets FIPS 140-2 level 3 requirements.
- Issuing CAs keys: The HSM used for CA keys meets FIPS 140-2 level 3 requirements.
- Subscriber keys: The HSM used Remote electronic signature keys meets FIPS 140-2 level 3 and EAL4+ requirements.

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

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

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

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

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

- Issuing CAs keys Management access to these keys is only possible using '4-eye' principle (2 out of 6).

- Subscriber keys on remote QSCD: Management access to these keys is only possible using '4-eye' principle (2 out of 6). Once the subscriber keys are generated, signing operations can be authorized by the Authenticated Subscriber (Login + PIN code + OTP).

6.2.3 PRIVATE KEY ESCROW

TunTrust does not escrow Private Keys for any reason.

6.2.4 PRIVATE KEY BACKUP

TunTrust creates backup copies of CA private keys and Subscriber private keys generated and stored by a Remote QSCD, for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices under the same multi-person control as the original Private Key.

Cryptographic modules used for private key storage meet the requirements of this CP/CPS. Private keys are copied to backup hardware cryptographic modules in accordance with this CP/CPS.

6.2.5 PRIVATE KEY ARCHIVAL

TunTrust does not archive Subscriber Private Keys.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

TunTrust CAs Private Keys are generated, activated and stored in Hardware Security Modules.

Private Keys are exported from the HSM only for backup purposes. Private keys are transferred between HSMs according to manufacturer's specifications, and only leave the originating device in encrypted form.

When transported between cryptographic modules, TunTrust encrypts the private key and protects the keys used for encryption from disclosure.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

TunTrust stores the CAs Private Keys on a FIPS 140-2 level 3 Hardware Security module which includes requirements to protect the Private Key and other assets against known threats.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

TunTrust is responsible for activating the Private Key in accordance with the instructions and documentation provided by the manufacturer of the hardware security module.

The following list shows how private keys are activated:

- Root CA keys: The Root CA keys are activated with three user keys (physical) and three user PINs (knowledge).
- Issuing CA keys: The Issuing CA keys are activated with two user keys (physical) and two user PINs (knowledge).
- Subscriber Private Keys on Remote QSCD: The Subscriber private key is protected by username, PIN and OTP codes.

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

TunTrust deactivates access to its CA Private Keys and stores its cryptographic modules in a secure safe when not in use. TunTrust never leaves its HSM devices in an active unlocked or unattended state. The method specified in Section 6.2.9 is operated for re-activation of private key.

Subscriber private keys may be deactivated after each operation, upon logging off their system, upon removal of the Local QSCD from the system, or upon logging off of the Remote QSCD. In all cases, Subscribers have an obligation to adequately protect their private key(s) in accordance with this CP/CPS.

6.2.10 METHOD OF DESTROYING PRIVATE KEY

TunTrust Private Keys are destroyed when they are no longer needed or when the Certificates to which they correspond have expired or have been revoked. Destroying Private Keys means that:

- TunTrust destroys all associated CA secret activation data in such a manner that no information can be used to deduce any part of the Private Key.
- TunTrust initializes the Hardware Security Module according to the specifications of the hardware manufacturer. In cases when this initialization procedure fails, TunTrust will physically destroy the device to remove the ability to extract any private key.

6.2.11 CRYPTOGRAPHIC MODULE RATING

See Section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 PUBLIC KEY ARCHIVAL

Public keys, in the form of certificates and certificate requests are archived as per Section 5.5.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

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

- The "**MOBILE ID ROOT CA"** is valid for 35 years from July 27th ,2023 to July 27th, 2058.
- The "**MODILE ID ISSUER CA**" is valid 30 years from issuing CAs July 27th ,2023 to July 27th, 2053.
- The end-user certificates can have a lifetime of 5 years.

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, shall represent an additional day.

6.4 Activation data

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

TunTrust activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. Generation and use of CA activation data used to activate CA Private Keys are made during a key ceremony. Activation data is assigned to shareholders in trusted roles as specified in Section 5.2.1. The cryptographic hardware is held under two-person control as explained in Section 5.2.2.

Activation data used (username, PIN and OTP) to protect Remote QSCD containing Subject's private keys are generated in accordance with the compliance requirements of the QSCD.

6.4.2 ACTIVATION DATA PROTECTION

TunTrust CAs activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms. TunTrust Activation data is protected via FIPS 140-2 Level 3 devices and may only be used via registered data entry devices.

TunTrust implements processes to temporarily lock access to TunTrust CA processes if a certain number of failed log-in attempts occur.

TunTrust Shareholders are required to safeguard their Secret Shares and remote QSCD Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

TunTrust implements processes to temporarily lock access to TunTrust CA processes if a certain number of failed log-in attempts occur.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

TunTrust CAs activation data are only held by TunTrust personnel in trusted roles as specified in Section 5.2.1.

6.5 Computer security controls

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

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

- Strong identification and authentication for all accounts capable of directly causing Certificate Issuance (physical access control to enter in the room by ID badge and PIN + logical control by certificate to access the system);
- User rights management (to implement the access control policy defined by TunTrust CA, to implement the principles of least privilege, multiple controls and separation of roles);
- Protection against computer viruses and other forms of compromise or unauthorized software and software updates from a trusted software repository;
- Security patches are applied within six (6) months of the security patch's availability, unless TunTrust documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch;
- Manage user accounts, including changes and the rapid removal of access rights;
- Network protection against intrusion of an unauthorized person using the firewall;
- Systems are segmented into networks based on their functional, or logical relationship;
- Networks are configured with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations
- Secure and encrypted communication between systems;
- Monitoring and audit procedures of the system configuration, including routing elements, are in place.

6.5.2 COMPUTER SECURITY RATING

TunTrust has established a security framework which covers and governs the technical aspects of its computer security.

As described in Section 5.4.8, the systems themselves and the services running on these systems are subject to thorough reviews and testing (including penetration testing).

TunTrust operates also a vulnerability management process which includes monitoring of supplier security alerts.

The technical aspects of computer security are subject to periodic audits.

6.6 Life cycle technical controls

6.6.1 SYSTEM DEVELOPMENT CONTROLS

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

Change requests require the approval of the change manager. Significant changes require the approval of TunTrust Board of Directors. All changes made to the CA systems are logged and tested before deployment.

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

All acquisitions made by TunTrust follow the Tunisian national law for governmental procurements. This includes the publication of request for proposals and evaluating each proposal (thus each vendor) according to the set specifications.

All hardware and software are shipped under standard conditions with controls in place to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering. Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors. Updates of equipment or software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel.

6.6.2 SECURITY MANAGEMENT CONTROLS

TunTrust establishes mechanisms to document, control, monitor, and maintain the security-related configurations and the integrity software, firmware and hardware of its CA systems, including any modifications or upgrades. The TunTrust CA's monitoring control processes includes issuance of alerts automatically and in real time when any changes are detected.

6.6.3 LIFE CYCLE SECURITY CONTROLS

TunTrust applies recommended security patches to Certificate Systems within six months of the security patch's availability, unless it documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

TunTrust does one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by TunTrust CA's vulnerability correction process:

1. Remediate the Critical Vulnerability;
2. If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to (1) vulnerabilities with high CVSS scores, starting with the vulnerabilities TunTrust determines are the most critical (such as those with a CVSS score of 10.0) and (2) systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or

3. Document the factual basis for the TunTrust determination that the vulnerability does not require remediation because (a) TunTrust disagrees with the NVD rating, (b) the identification is a false positive, (c) the exploit of the vulnerability is prevented by compensating controls or an absence of threats; or (d) other similar reasons.

6.7 Network security controls

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

TunTrust maintains the Root CA Systems in a High Security Zone. TunTrust Root CAs Keys are kept offline and brought on-line only when necessary to sign certificate-issuing subordinate CAs or periodic CRLs or OCSP certificates.

Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. It is TunTrust 's security policy to block all ports and protocols and open only necessary ports to enable CA functions.

All CA equipment is configured with a minimum number of services and accounts and all unused network ports, accounts and services are disabled. All firewall configurations and changes thereto are documented, authorized and implemented in accordance with change management procedures. Changes to network configuration policy go through the same change management process as host devices, and are similarly documented, reviewed and approved.

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

TunTrust implements automated mechanisms under the control of TunTrust trusted roles to process logged system activity and alert multiple destinations of possible Critical Security Events. TunTrust requires trusted role personnel to follow up on alerts of possible Critical Security Events.

6.8 Time-Stamping

All TunTrust CA components are regularly synchronized with a reliable time service. TunTrust CA uses a GPS-NTP time source to establish the correct time for:
- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates; and
- Issuance of Subscriber end entity Certificates.

7 CERTIFICATE PROFILE

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

7.1 Certificate Profile

TunTrust generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

- The profiles of TunTrust CAs certificates are described in Appendix A of this CP/CPS.
- The profiles of Subscribers certificates are described in Appendix B of this CP/CPS.

7.1.1 VERSION NUMBER(S)

TunTrust CAs issue X.509 version 3 certificates.

7.1.2 CERTIFICATE CONTENT AND EXTENSIONS; APPLICATION OF RFC 5280

X.509 v3 extensions are supported and used for Certificate profiles as described in Appendix A and Appendix B.

7.1.2.1 ROOT CA CERTIFICATE

See Appendix A.

7.1.2.2 7.1.2.2   SUBORDINATE CA CERTIFICATE

See Appendix A.

7.1.2.3 SUBSCRIBER CERTIFICATE

See Appendix B.

7.1.2.4 ALL CERTIFICATES

All fields and extensions in TunTrust Certificates are set in accordance with RFC 5280. See Appendix A and Appendix B.

TunTrust does not issue a Certificate with:

a. extensions that do not apply in the context of the public Internet (such as an extKeyUsage value for a service that is only valid in the context of a privately managed network), unless:

   i. such value falls within an OID arc for which the Applicant demonstrates ownership, or

   ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or

b. semantics that, if included, will mislead a Relying Party about the Certificate information verified by the CA (such as including extKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.2.5 APPLICATION OF RFC 5280

For purposes of clarification, a Pre-certificate, as described in RFC 6962 – Certificate Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key

Infrastructure Certificate and Certificate Revocation List (CRL) Profile under the current Baseline Requirements.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

All signing algorithms used by TunTrust are sha256ECDSA, sha384ECDSA and sha512ECDSA. TunTrust CA does not, and never has, used SHA-1 as a component of any signature algorithm on a certificate.

Algorithms OID are conforming to IETF RFC 3279 and RFC 5280.

7.1.3.1 SUBJECTPUBLICKEYINFO

TunTrust indicates an ECDSA key using the ecdsaEncryption (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters are present, and are an explicit NULL.

When encoded, the `AlgorithmIdentifier` for ECDSA keys are:

- For P-256 keys, 301306072a8648ce3d020106082a8648ce3d030107.
- For P-384 keys, 301006072a8648ce3d020106052b81040022.
- For P-521 keys, 301006072a8648ce3d020106052b81040023.

7.1.3.2 SIGNATURE ALGORITHMIDENTIFIER

All objects signed by a TunTrust CA Private Key MUST conform to the CA/B Forum Baseline Requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

No other encodings are permitted for these fields.

When encoded, the `AlgorithmIdentifier` is byte-for-byte identical with the specified hex-encoded bytes:

- If the signing key is P-256, the signature MUST use ECDSA with SHA-256. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040302.
- If the signing key is P-384, the signature MUST use ECDSA with SHA-384. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040303.
- If the signing key is P-521, the signature MUST use ECDSA with SHA-512. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040304.

TunTrust does not sign SHA-1 hashes over :

- certificates with an EKU extension containing the id-kp-ocspSigning key purpose;
- "MOBILE ID ROOT CA" Certificates;
- "MOBILE ID ISSUER CA" Certificates;
- OCSP responses; or
- CRLs.

7.1.4 NAME FORMS

7.1.4.1 ISSUER INFORMATION

Name forms are in the X.500 distinguished name form as implemented in RFC 3739. The content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, Section 4.1.2.4.

7.1.4.2 SUBJECT INFORMATION – SUBSCRIBER CERTIFICATES

Subject attributes don't contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.3 SUBJECT INFORMATION – ROOT CERTIFICATES AND SUBORDINATE CA CERTIFICATES

By issuing a Subordinate CA Certificate, TunTrust represents that it followed the procedure set forth in its CP/CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.5 NAME CONSTRAINTS

TunTrust CAs are technically unconstrained and are subject for full audit as specified in Section 8 of this CP/CPS.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

7.1.6.1 RESERVED CERTIFICATE POLICY IDENTIFIERS

TunTrust does not issue SSL certificates under this hierarchy of CAs.

7.1.6.2 ROOT CA CERTIFICATES

MOBILE ID ROOT CA Certificate do not contain any certificatePolicies extension, therefore do not have policy identifiers in them.

7.1.6.3 SUBORDINATE CA CERTIFICATES

The OIDs of TunTrust Subordinate CAs are listed in Section 1.3 of this CP/CPS.

7.1.6.4 SUBSCRIBER CERTIFICATES

The certificate policy identifiers of the Subscriber Certificates are listed in Appendix B.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

Since the pathLenConstraint is set to zero, no policy constraints were placed on the Issuing CA.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

TunTrust does not include anything in the Policy Qualifier field of the certificate Policies extension.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

The certificate policies extension is set to non-critical in TunTrust CAs and Subscribers certificates.

7.2 CRL profile

7.2.1 VERSION NUMBER(S)

TunTrust CAs issue X.509 Version 2 CRLs in accordance with IETF PKIX RFC 5280.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

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

The encoding of the Issuer field in the CRL is byte-for-byte equivalent with the encoding of the Issuer in the certificate; that is, using the exact same string types and field contents. The extension reasonCode (OID 2.5.29.21) is present and is marked critical.

The CRLReason indicated MUST NOT be unspecified (0). If the reason for revocation is unspecified, TunTrust Issuing CAs MUST omit reasonCode entry extension, if allowed by the previous requirements.

The CRLReason indicated is not in any case certificateHold (6).

If a reasonCode CRL entry extension is present, the CRLReason MUST indicate the most appropriate reason for revocation of the certificate.

TunTrust CRL profiles description is available in Appendix C of this CP/CPS.

7.3 OCSP profile

The TunTrust OCSP functionality is built according to RFC 6960.

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

If an OCSP response is for a Root CA and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus is present.

The CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 VERSION NUMBER

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

7.3.2 OCSP EXTENSION

TunTrust OCSP profile description is available in Appendix D of this CP/CPS.

The singleExtensions of an OCSP response does not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8   COMPLIANCE AUDIT AND OTHER ASSESSMENTS

TunTrust is a government entity licensed by Tunisian Law to act as a National Certification Authority, TunTrust operates at all times in compliance to the following:

A. the applicable laws;

B. the requirements of this CP/CPS;

C. the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates of the CA/B Forum; and

D. the latest versions of ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2.

8.1   Frequency or circumstances of assessment

An annual audit is performed by an independent external auditor to assess TunTrust's compliance with standards set forth above.

An audit period must not exceed one year in duration. In addition to that, more than one compliance audit per year is possible if this is requested by TunTrust or is a result of unsatisfactory results of a previous audit.

8.2   Identity/qualifications of assessor

TunTrust's audit is performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.1 of the CA/B Forum Baseline Requirements);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function; and
4. accredited in accordance with ISO17065 applying the requirements specified in ETSI EN 319 403;
5. Bound by law, government regulation, or professional code of ethics.

8.3   Assessor's relationship to Assessed Entity

TunTrust utilizes independent auditors that do not have any financial interest or business relationship that could foreseeably create a significant bias for or against TunTrust.

8.4   Topics covered by assessment

TunTrust undergoes an audit in accordance with the current versions of ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI EN 319 401. Topics covered in this annual audit include, but are not limited to, the requirements of this CP/CPS, environmental controls, CA key management, and certificate life cycle management.

The chosen audit scheme incorporates periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit is conducted by a Qualified Auditor, as specified in Section8.2.

8.5 Actions taken as a result of deficiency

With respect to compliance audits of TunTrust's operations, significant exceptions or deficiencies identified during the compliance audit will result in a determination of actions to be taken. This determination is made by TunTrust Board of Directors with input from the auditor. If exceptions or deficiencies are identified, TunTrust management is responsible for developing and implementing a corrective action plan. Once the plan has been implemented, TunTrust will call for an auxiliary audit to verify that the noted deficiencies have been remediated.

8.6 Communication of results

TunTrust makes the Audit Report publicly available at https://www.tuntrust.tn/repository. The results will also be sent to any other appropriate entities that may be entitled by law, regulation, or agreement to receive a copy of the audit results.

TunTrust makes its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, TunTrust will provide an explanatory letter signed by the Qualified Auditor.

For Audit Reports in which the Audit Period includes a date later than 2020-08-01, then the requirements set forth in the remainder of this Section SHALL be met. Audit Reports for Audit Periods that conclude prior to 2020-08-01 SHOULD meet these requirements.

The Audit Report contains at least the following clearly-labeled information:

1. name of the organization being audited;

2. name and address of the organization performing the audit;

3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, that were in-scope of the audit;

4. audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);

5. a list of the CA policy documents, with version numbers, referenced during the audit;

6. whether the audit assessed a period of time or a point in time;

7. the start date and end date of the Audit Period, for those that cover a period of time;

8. the point in time date, for those that are for a point in time;

9. the date the report was issued, which will necessarily be after the end date or point in time date;

10. a statement to indicate if the audit was a full audit or a surveillance audit, and which portions of the criteria were applied and evaluated, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part 1 (General Requirements), and/or Part 2 (Requirements for Trust Service Providers).

11. a statement to indicate that the auditor referenced the applicable CA/Browser Forum criteria, such as this document, and the version used.

An authoritative English language version of the publicly available audit information MUST be provided by the Qualified Auditor and TunTrust will ensure it is publicly available.

The Audit Report MUST be available as a PDF, and SHALL be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report MUST be uppercase letters and MUST NOT contain colons, spaces, or line feeds.

8.7 Self-Audits

TunTrust performs regular internal audits of its operations, personnel, and compliance with this CP/CPS.

During the period in which TunTrust issues Certificates, TunTrust monitors adherence to this CP/CPS and the CA/B Forum requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one Certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9   OTHER BUSINESS AND LEGAL MATTERS

9.1   Fees

9.1.1   CERTIFICATE ISSUANCE OR RENEWAL FEES

TunTrust does not charges fees for issuing of subject's certificates.

9.1.2   CERTIFICATE ACCESS FEES

TunTrust does not charge fees for access to its certificate databases.

9.1.3   REVOCATION OR STATUS INFORMATION ACCESS FEES

TunTrust does not charge a Certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL or the OCSP.

9.1.4   FEES FOR OTHER SERVICES

TunTrust may elect to charge for its other services. Such fees will be outlined in the applicable Subscriber agreement.

9.1.5   REFUND POLICY

TunTrust does not refund the fees of Certificates.

9.2   Financial responsibility

9.2.1   INSURANCE COVERAGE

TunTrust currently maintains a commercial general liability insurance according to the National Law.

9.2.2   OTHER ASSETS

Since TunTrust is a governmental entity, it shall have access to other resources to support operations and pay damages for potential liability, which may be couched in terms of a minimum level of assets necessary to operate and cover contingencies that might occur within TunTrust PKI.

9.2.3   INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

No warranty coverage is available for Subscribers and Relying Parties except the warranties listed in Section 9.6.1.

9.3   Confidentiality of business information

9.3.1   SCOPE OF CONFIDENTIAL INFORMATION

TunTrust keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel. Confidential information includes, but is not limited to:

- Private Keys;
- Activation data used to access Private Keys or to gain access to the CA system;
- Disaster Recovery, and Business Continuity Plans;
- Any certificate application records and documentation submitted in support of Certificate Applications, which is not in relation to an issued certificate, whether successful or rejected;
- External or internal audit trail records and reports, which are not required to be openly published;
- Transaction records, financial audit records, and internal records on the operations of TunTrust's infrastructure, certificate management, services and data.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

The following are not considered confidential:

1. Certificates;

2. Certificate revocation Lists;

3. CP/CPS; and

4. any information available in TunTrust repository at https://www.tuntrust.tn/repository.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

TunTrust protects and secures confidential information from disclosure. All employees of TunTrust are bound by TunTrust Information Security Policy and required by the security chart engagements to preserve the confidentiality of information so labelled.

9.4 Privacy of personal information

9.4.1 PRIVACY PLAN

TunTrust protects personal information in accordance with the Tunisian law N° 2004-63 of July 27th, 2004 on the protection of personal data and TunTrust internal document.

TunTrust makes available to Subscribers and Relying Parties its Privacy Policy on the website https://www.tuntrust.tn/repository .

9.4.2 INFORMATION TREATED AS PRIVATE

TunTrust treats all personal information about an individual that is not publicly available in the contents of a Certificate, CRL or OCSP as private information. TunTrust protects private information using appropriate safeguards and a reasonable degree of care.

9.4.3 INFORMATION NOT DEEMED PRIVATE

Private information does not include Certificates, CRLs, or their contents and the personal or corporate information appearing in them.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

TunTrust employees and contractors are expected to handle personal information in strict confidence and meet the requirements of Tunisia law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

Personal information obtained from an Applicant during the application or identity verification process is considered private information if the information is not included in a Certificate. As part of a Subscriber Agreement, all Subscribers consent to the global transfer of any personal data contained in the Certificate and agree to allow TunTrust to handle any private information required for the issuance and maintenance of certificates.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

TunTrust will only release or disclose private information on judicial or other authoritative order.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

TunTrust is not required to release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by a legal entity as stated in Section 9.4.6.

9.5 Intellectual property rights

TunTrust does not knowingly violate the intellectual property rights of third parties. Public and Private Keys remain the property of Subscribers who legitimately hold them.

TunTrust owns the intellectual property rights in TunTrust's services, including the certificates, trademarks used in providing the services, and this CP/CPS. Certificate and revocation information are the property of TunTrust.

TunTrust grants permission to reproduce and distribute Certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

9.6 Representations and warranties

9.6.1 CA REPRESENTATIONS AND WARRANTIES

By issuing a Certificate, TunTrust makes the Certificate warranties listed herein to the following Certificate beneficiaries:

- The Subscriber that is a party to the Subscriber Agreement;

- All Application Software Suppliers with whom TunTrust has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and

- All Relying Parties who reasonably rely on a Valid Certificate.

TunTrust represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, TunTrust has complied with the CA/B Forum Baseline Requirements and its Certificate Policy / Certification Practice Statement in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. **Authorization for Certificate:** That, at the time of issuance, TunTrust (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
2. **Accuracy of Information:** That, at the time of issuance, TunTrust and the DRA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
3. **No Misleading Information:** That, at the time of issuance, TunTrust (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
4. **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, TunTrust (i) implemented a procedure to verify the identity of the Applicant in accordance with Section3.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
5. **Subscriber Agreement:** That, if TunTrust and the Subscriber are not Affiliated, the Subscriber and TunTrust are parties to a legally valid and enforceable Subscriber Agreement that satisfies the CA/B Forum Baseline Requirements, or, if TunTrust and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
6. **Status:** That TunTrust maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
7. **Revocation:** That TunTrust will revoke the Certificate for any of the reasons specified in the CA/B Forum Baseline Requirements.
8. **Access to Remote QSCD**: TunTrust ensures the access to the private keys on the Remote QSCD to the authorized Subscriber of the keys and the proper management and compliance of the Remote QSCD.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

TunTrust DRA represents that:
1. Information provided by the DRA does not contain any false or misleading information,
2. Translations performed by the DRA are an accurate translation of the original information, and
3. All Certificates requested by the DRA meet the requirements of the applicable CP/CPS.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

TunTrust requires, as part of the Subscriber Agreement, that the Applicant makes the commitments and warranties in this Section for the benefit of TunTrust and the Certificate Beneficiaries.
Prior to the issuance of a Certificate, TunTrust obtains, for the express benefit of TunTrust and the Certificate Beneficiaries, the Applicant's agreement to the Subscriber Agreement with TunTrust CA.

TunTrust implements a process to ensure that each Subscriber Agreement is legally enforceable against the Applicant. In either case, the Agreement is applied to the Certificate to be issued pursuant to the Certificate request.

A separate Agreement is used for each Certificate request, or a single Agreement is used to cover multiple future Certificate requests and the resulting Certificates, as long as each Certificate that TunTrust issues to the Applicant is clearly covered by that Subscriber Agreement.

The Subscriber Agreement contains provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to TunTrust, both in the Certificate request and as otherwise requested by TunTrust in connection with the issuance of the Certificate(s) to be supplied by TunTrust;

2. **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);

3. **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;

4. **Use of Certificate:** An obligation and warranty to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement;

5. **Reporting and Revocation:** An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.

6. **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.

7. **Responsiveness:** An obligation to respond to TunTrust's instructions concerning Key Compromise or Certificate misuse within a specified time period.

8. **Acknowledgment and Acceptance:** An acknowledgment and acceptance that TunTrust is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or if revocation is required by the present CP/CPS, or the CA/B Forum Baseline Requirements.

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

Each Relying Party represents that, prior to relying on a TunTrust Certificate, it:

1. Obtained sufficient knowledge on the use of digital Certificates and PKI,

2. Studied the applicable limitations on the usage of Certificates and agrees to TunTrust's limitations on liability related to the use of Certificates,

3. Has read, understands, and agrees to this CP/CPS,

4. Verified both the TunTrust Certificate and the Certificates in the certificate chain using the relevant CRL or OCSP,

5. Will not use a TunTrust Certificate if the Certificate has expired or been revoked, and

6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a TunTrust Certificate after considering:

a) applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction,

b) the intended use of the Certificate as listed in the Certificate or this CP/CPS,

c) the data listed in the Certificate,

d) the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,

e) the Relying Party's previous course of dealing with the Subscriber,

f) the Relying Party's understanding of trade, including experience with computer-based methods of trade, and

g) any other indication of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a Certificate is at a party's own risk.

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

No implied or express warranties are given by TunTrust to other participants other than in Subscriber agreements, Relying Party agreements and any other agreements signed by TunTrust with Third Parties.

9.7 Disclaimers of warranties

To the extent permitted by applicable law, this CP/CPS, the Subscriber Agreement, the Relying Party Agreement and any other contractual agreement applicable within the TunTrust PKI shall disclaim TunTrust possible warranties, including any warranty of merchantability or fitness for a particular purpose.

To the extent permitted by applicable law, TunTrust makes no express or implied representations or warranties pursuant to this CP/CPS. TunTrust expressly disclaims any and all express or implied warranties of any type to any person, including any implied warranty of title, non-infringement, merchantability, or fitness for a particular purpose.

9.8 Limitations of Liability

TunTrust is only liable for damages which are the result of its failure to comply with this CP/CPS and which were provoked deliberately or wantonly negligent.

TunTrust is not in any event be liable for any loss of profits, indirect and consequential damages, or loss of data, to the extent permitted by applicable law. TunTrust is not liable for any damages resulting from infringements by the Subscriber or the Relying Party on the applicable terms and conditions.

TunTrust is not in any event liable for damages that result from force major events as detailed in Section9.5. TunTrust takes commercially reasonable measures to mitigate the effects of force major in due time. Any damages resulting of any delay caused by force major will not be covered by TunTrust.

The Subscriber is liable to TunTrust and Relying Parties for any damages resulting from misuse, willful misconduct, failure to meet regulatory obligations, or noncompliance with other provisions for using the Certificate.

9.9 Indemnities

9.9.1 INDEMNIFICATION BY TUNTRUST

Notwithstanding any limitations on its liability to Subscriber and Relying Parties, TunTrust acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with TunTrust do not assume any obligation or potential liability of TunTrust under this CP/CPs or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. TunTrust shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by TunTrust, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by TunTrust where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from TunTrust online, and the application software either failed to check such status or ignored an indication of revoked status).

Additional indemnity provisions and obligations are contained within relevant contractual agreements such as the Subscriber Agreement and Relying Party Agreement.

9.9.2 INDEMNIFICATION BY SUBSCRIBERS

To the extent permitted by law, each Subscriber shall release, indemnify and hold harmless TunTrust CA, and all TunTrust directors, shareholders, officers, agents, employees, contractors and successors of the foregoing, against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of its Subscriber Agreement, this CP/CPS, or applicable law; (iii) the compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of a certificate or Private Key.

9.9.3 INDEMNIFICATION BY RELYING PARTIES

To the extent permitted by law, each Relying Party shall release, indemnify and hold harmless TunTrust CA, and all TunTrust directors, shareholders, officers, agents, employees, contractors and successors of the foregoing against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of any service terms applicable to the services provided by TunTrust or its affiliates and used by the Relying Party, this CP/CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.10 Term and termination

9.10.1 TERM

This CP/CPS, and any amendments thereto, are effective upon publication in TunTrust's Repository.

9.10.2 TERMINATION

This CP/CPS, as may be amended from time to time, are effective until replaced by a new version, which shall be published in TunTrust's Repository.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon Termination of this CP/CPS, Subscribers, and Relying Parties are bound by its terms for all Certificates issued, while it's effective, for the remainder of the validity periods of such Certificates.

9.11 Individual notices and communications with participants

TunTrust, Subscribers, Applicants, Relying Parties and other participants will use official means of communication in public service as per Tunisia National Law.

9.12 Amendments

9.12.1 PROCEDURE FOR AMENDMENT

This CP/CPS is reviewed at least annually and may be reviewed more frequently. Revisions of this CP/CPS are reviewed and approved within TunTrust Board of Directors. Amendments are made by posting an updated version of the CP/CPS to the online repository. Changes to this CP/CPS are indicated by an incremental version number.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

Updates, amendments, and new versions of TunTrust's CP/CPS shall be posted in TunTrust's repository. Such publication shall serve as notice to all relevant entities.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

If TunTrust's Board of Directors determines that a change is necessary in the object identifier corresponding to this CP/CPS, the amendment shall contain new object identifiers for this CP/CPS. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 Dispute resolution provisions

Parties are required to notify TunTrust and attempt to resolve disputes directly with TunTrust before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14 Governing law and place of jurisdiction

This CP/CPS is governed, construed and interpreted in accordance with the laws of Tunisia. This choice of law is made to ensure uniform interpretation of this CP/CPS, regardless of the place of residence or place of use of TunTrust Certificates. The law of Tunisia applies also to all TunTrust commercial or contractual relationships in which this CP/CPS may apply or quoted implicitly or explicitly in relation to TunTrust products and services where TunTrust acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including TunTrust partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Ariana in Tunisia.

9.15 Compliance with applicable law

TunTrust is subject to all national applicable laws of Tunisia.

9.16 Miscellaneous provisions

9.16.1 ENTIRE AGREEMENT

This CP/CPS and the applicable Subscriber Agreement and Relying Party Agreement represent the entire agreement between any Subscriber or Relying Party and TunTrust and shall supersede any and all prior understandings and representations pertaining to its subject matter. In the event, however, of a conflict between this CP/CPS and any other express agreement between a Subscriber or Relying Party with TunTrust with respect to a Certificate, including but not limited to a Subscriber Agreement or the Relying Party Agreement, such other agreement shall take precedence.

9.16.2 ASSIGNMENT

Entities operating under this CP/CPS cannot assign their rights or obligations without the prior written consent of TunTrust.

9.16.3 SEVERABILITY

In the event of a conflict between the CA/B Forum Baseline Requirements and a Tunisian law, regulation or government order, TunTrust may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in Tunisia.
This applies only to operations or certificate issuances that are subject to that Law. In such event, TunTrust will immediately (and prior to issuing a certificate under the modified requirement) include in this Section a detailed reference to the Law requiring a modification of the CA/B Forum Baseline Requirements under this Section, and the specific modification to the Baseline Requirements implemented by TunTrust.
TunTrust will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CP/CPS.

Any modification to TunTrust practice enabled under this Section will be discontinued if and when the Law no longer applies, or the Baseline Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CP/CPS and a notice to the CA/Browser Forum, as outlined above, is made within 90 days.

9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)

TunTrust may seek indemnification and any fees (including reasonable attorney's fees and court costs) from a party for damages, losses and expenses related to that party's conduct.

The waiver or failure to exercise any right provided for in this CP/CPS shall not be deemed a waiver of any further or future right under this CP/CPS.

9.16.5 FORCE MAJEURE

TunTrust is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by an occurrence beyond TunTrust's reasonable control. The operation of the Internet is beyond TunTrust's reasonable control.

9.17 Other provisions

The present CP/CPS does not state any conditions in this respect.

APPENDIX A: MOBILE ID PKI CERTIFICATE PROFILES

1. MOBILE ID ROOT CA

The following table describes the certificate profile of "**MOBILE ID ROOT CA**":

Fields	Critical	Values
Version		3 (0x2)
Serial Number		7a:69:0c:78:2f:f9:f6:ef
Signature Algorithm		ecdsa-with-SHA512
Issuer		CN=MOBILE ID ROOT CA, O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE, C=TN
Validity		
Not Before		Jul 27 08:22:21 2023 GMT
Not After		Jul 27 08:22:21 2058 GMT
Subject		CN=MOBILE ID ROOT CA, O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE, C=TN
Subject Public Key Info		
Public Key Algorithm		id-ecPublicKey
RSA Public Key		512 bits
X509v3 extensions		
X509v3 Subject Key Identifier		0C:31:2F:41:13:74:C3:19:A8:03:05:2B:10:C1:C2:B4:74:D6:E5:4C
X509v3 Basic Constraints	True	CA: TRUE
X509v3 Authority Key Identifier		Keyid: 0C:31:2F:41:13:74:C3:19:A8:03:05:2B:10:C1:C2:B4:74:D6:E5:4C
X509v3 Key Usage	True	Certificate Sign, CRL Sign
Signature Algorithm		ecdsa-with-SHA512

2. MOBILE ID ISSUER CA

The following table describes the certificate profile of MOBILE ID ISSUER CA:

Fields	Critical	Values
Version		3 (0x2)
Serial Number		1d:7f:54:02:88:92:33:1a
Signature Algorithm		ecdsa-with-SHA384
Issuer		CN=MOBILE ID ROOT CA, O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE, C=TN
Validity		
Not Before		Jul 27 09:11:32 2023 GMT
Not After		Jul 27 09:11:32 2053 GMT
Subject		CN=MOBILE ID ISSUER CA, O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE, C=TN
Subject Public Key Info		
Public Key Algorithm		id-ecPublicKey
RSA Public Key		384 bits
X509v3 extensions		
Authority Information Access		CA Issuers - URI: http://www.tuntrust.tn/pub/mobileidrootca.crt OCSP - URI: http://va.tuntrust.tn
X509v3 Subject Key Identifier		57:DE:C6:A7:31:50:D4:A4:F7:DE:EE:9C:A0:3A:2F:74:BC:FE:99:F8
X509v3 Basic Constraints	True	CA:TRUE
X509v3 Authority Key Identifier		Keyid: 0C:31:2F:41:13:74:C3:19:A8:03:05:2B:10:C1:C2:B4:74:D6:E5:4C
X509v3 Certificate Policies		Policy: 2.16.788.1.2.7.1.3.1
X509 CRL Distribution Points		URI: http://crl.tuntrust.tn/mobileidrootca.crl
X509v3 Key Usage	True	Certificate Sign, CRL Sign
Signature Algorithm		ecdsa-with-SHA384

APPENDIX B : MOBILE ID PKI END-ENTITY PROFILES

The following table provides the description of the fields for Mobile ID Certificate issued under "**MOBILE ID ISSUER CA**".

Base Profile	Included	Critical	O/M[1]	CO[2]	Values
Data:					
Version	X	False	M	S	3 (0x2)
Serial Number	X	False	M	FDV	Validated on duplicates
Signature Algorithm	X	False	M	S	ecdsa-with-SHA256
Issuer	X	False	M	S	CN=MOBILE ID ISSUER CA, O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE, C=TN
Validity					
Not Before	X	False	M	D	Certificate generation process date/time
Not After	X	False	M	D	Certificate generation process date/time + 5 years.
Subject					
C, countryName	X	False	M	D	Nationality of the holder (ISO3166).
surname	X	False	M	D	Surname as on ID card.
givenName	X	False	M	D	Given Name as on ID card without indication of 'بنت', 'حرم' or similar.
CN, commonName	X	False	M	D	Concatenation of given name and surname as in ID card separated by a "space" character without indication of 'حرم', 'بنت' or similar.

---

1. O/M: O = Optional, M = Mandatory.

2. CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

SerialNumber	X	False	M	D	Concatenation of « PNO », country code « TN », « - » and the digital identifier of the citizen.
Subject Public Key Info:					
Public Key Algorithm	X	False	M	S	id-ecPublicKey
Public-Key	X	False	M	S	(256 bit)
X509v3 extensions					
X509v3 Basic Constraints:	X	True	M	S	CA:False
X509v3 Authority Key Identifier	X	False	M	S	57:DE:C6:A7:31:50:D4:A4:F7:DE:EE:9C:A0:3A:2F:74:BC:FE:99:F8
Authority Information Access	X	False	M	S	CA Issuers - URI: http://www.tuntrust.tn/pub/mobileidissuerca.crt OCSP – URI : http://va.tuntrust.tn
X509v3 Certificate Policies	X	False	M	S	Policy : 0.4.0.2042.1.2 Policy : 2.16.788.1.2.7.1.3.1.1 Policy : 0.4.0.194112.1.2
X509v3 Extended Key Usage	X	False	M	S	TLS Web Client Authentication, E-mail Protection, Microsoft Document Signing
X509v3 CRL Distribution Points	X	False	M	S	Full Name : URI: http://crl.tuntrust.tn/mobileidissuerca.crl
X509v3 Subject Key Identifier:	X	False	M	D	SHA-1 Hash of subject key
X509v3 Key Usage	X	True	M	S	Digital Signature, Non Repudiation

qcStatements					QcCompliance (0.4.0.1862.1.1) QcSSCD (0.4.0.1862.1.4) QcPDS (0.4.0.1862.1.5): https://www.tuntrust.tn/pub/pds-mobileidissuerca.pdf QcType (0.4.0.1862.1.6 0.4.0.1862.1.6.1)

APPENDIX C : MOBILE ID PKI CAS CRL PROFILES

1. "MOBILE ID ROOT CA" CRL

The following table describes the CRL profile of "**MOBILE ID ROOT CA**":

Field	Value
Version	2 (0x1)
Signature Algorithm	ecdsa-with-SHA512
Issuer	/CN=MOBILE ID ROOT CA/O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE/C=TN
Last Update	CRL generation process date/time.
Next Update	CRL generation process date/time + 365 days
CRL extensions	
X509v3 Authority Key Identifier	0C:31:2F:41:13:74:C3:19:A8:03:05:2B:10:C1:C2:B4:74:D6:E5:4C
X509v3 CRL Number	A monotonically increasing sequence number
Revoked Certificates:	
Serial Number	Serial number of the revoked certificate
Revocation Date	Date and time of the revocation
CRL entry extensions:	
X509v3 CRL Reason Code	Code of Reason of revocation
Signature Algorithm	ecdsa-with-SHA512

2. "MOBILE ID ISSUER CA" CRL

The following table describes the CRL profile of "**MOBILE ID ISSUER CA**":

Field	Value
Version	2 (0x1)
Signature Algorithm	ecdsa-with-SHA384
Issuer	/CN=MOBILE ID ISSUER CA/O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE/C=TN
Last Update	CRL generation process date/time.
Next Update	CRL generation process date/time + 6 days
CRL extensions	
X509v3 Authority Key Identifier	57:DE:C6:A7:31:50:D4:A4:F7:DE:EE:9C:A0:3A:2F:74:BC:FE:99:F8
X509v3 CRL Number	A monotonically increasing sequence number
Revoked Certificates:	
Serial Number:	Serial number of the revoked certificate
Revocation Date	Date and time of the revocation
CRL entry extensions:	
X509v3 CRL Reason Code	Code of Reason of revocation
Signature Algorithm	ecdsa-with-SHA384

APPENDIX D: MOBILE ID PKI OCSP PROFILES

1. "MOBILE ID ROOT CA" OCSP Profile

Base Profile	Included	Critical	O/M[3]	CO[4]	Values
Version	X	False		S	Version: 3(0x2)
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	ecdsa-with-SHA512
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	Issuing CA DN
Subject DN	X	False			
commonName	X		M	D	Name of the validation Authority
countryName	X		M	D	Country in which the organization's registered office is established (ISO3166).
OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
Locality	X		O	D	Locality Name
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 730 days
subjectPublicKeyInfo	X	False			

---

3. O/M: O = Optional, M = Mandatory.

4. CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

Algorithm	X				Public Key: Key length: 512 bits (ECDSA)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				Authority Key Identifier
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA : FALSE
KeyUsage	X	True			
digitalSignature	X			S	True
OCSP No Check	X			S	
Extended Key Usage	X	False			
OCSP Signing	X			S	True

2. "MOBILE ID ISSUER CA" OCSP Profile

Base Profile	Included	Critical	O/M[5]	CO[6]	Values
Version	X	False		S	Version: 3(0x2)
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	ecdsa-with-SHA384
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	Issuing CA DN
Subject DN	X	False			

---

5. O/M: O = Optional, M = Mandatory.

6. CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

commonName	X		M	D	Name of the validation Authority
countryName	X		M	D	Country in which the organization's registered office is established (ISO3166).
OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
Locality	X		O	D	Locality Name
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 730 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 384 bits (ECDSA)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				Authority Key Identifier
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA : FALSE
KeyUsage	X	True			
digitalSignature	X			S	True
OCSP No Check	X			S	
Extended Key Usage	X	False			
OCSP Signing	X			S	True