Tunisian National PKI

Certificate Policy / Certification Practice Statement

Review

Version	Date	Comment	Section/Page
00	15/02/2017	1st Writing	Whole document
01	17/03/2017	1st revision	Section 1.1, 4.93, 4.12.1, 5.2.1, 6.2.3, 7.1
02	21/04/2017	2nd revision	Sections 1.1, 4.9.8, 7.1.2.1, 7.1.2.2, 7.4
03	27/11/2017	3rd revision	Sections 1.3.7
04	02/03/2018	4th revision	Sections 1.6, 3.2.3, 6.3.2
05	31/08/2018	5th revision	Update all sections
06	22/10/2018	6th revision	Sections 1.1 , 1.6.1, 1.3.2, 2.1 , 2.3, 2.4, 3.2.2.2, 3.2.2.4.1, 3.2.2.7, 3.2.3, 4.2.1, 4.9.10, 7.1.4.
07	08/01/2019	7th revision	Sections 1.1, 1.3, 1.5.1, 1.6, 2.3, 3, 4, 5, 6.1.6, 7.1, 8.0, 8.6 and 9
08	30/05/2019	8th revision	Sections 1, 2, 3, 4, 5, 7, 8 and 9
09	12/09/2019	9th revision	Sections 1, 2, 3, 4, 5, 7, 8 and 9

Approval of the document

	Author	Validated by	Approved by
Entity :	TunTrust	TunTrust Board of Directors	TunTrust Board of Directors
Date :	26/07/2019	10/09/2019	11/09/2019

Table of Contents

1 INTRODUCTION

1.1 Overview

The Agence Nationale de Certification Electronique was founded in accordance with Law no. 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", "TunTrust CA", "TnTrust CA" and "TunTrust PKI" are used interchangeably and include TunTrust Root CA and Issuing CAs 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.

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.

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 Tunisian National Root CA and its subordinate CAs 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.

The OID of the present document is: 2.16.788.1.2.6.1.9

Revisions of this document have been made as follows:

Date	Changes	Version
15/02/2017	The original CP/CPS document for public.	00
17/03/2017	Section 1.1, 4.93, 4.12.1, 5.2.1, 6.2.3, 7.1	01
21/04/2017	Sections 1.1, 4.9.8, 7.1.2.1, 7.1.2.2, 7.4	02

27/11/2017	Sections 1.3.7	03
02/03/2018	Sections 1.6, 3.2.3, 6.3.2	04
31/08/2018	Update all sections	05
22/10/2018	Sections 1.1 , 1.6.1, 1.3.2, 2.1 , 2.3, 2.4, 3.2.2.2, 3.2.2.4.1, 3.2.2.7, 3.2.3, 4.2.1, 4.9.10, 7.1.4.	06
08/01/2019	Sections 1.1, 1.3.2, 1.3.2.3, 1.5.1, 1.6, 2.3, 3.1.1, 3.1.5, 3.2, 3.2.1.1, 3.2.2.2, 3.2.2.4, 3.2.2.5, 3.2.2.7, 3.2.2.8, 3.2.3, 3.2.4, 3.2.5, 3.3.2, 4.2.1, 4.3.1, 4.4.1, 4.9, 4.9.3, 4.9.4, 4.9.5, 4.9.8, 5.2.1, 5.2.2, 5.4.1, 5.9.3, 6.1.6, 7.1, 7.1.4, 8.0, 8.6, 9.1.2, 9.3.1, 9.4.2 and 9.6.2.	07
30/05/2019	Sections 1.1, 1.3, 1.4, 1.5, 1.6, 2, 3.1, 3.2, 3.4, 4.3, 4.4, 4.5, 4.6, 4.8, 4.9, , 5.2.1. , 5.2.3, 5.3, 5.4.2, 5.4.7, 5.4.8, 5.5.2, 7.2, 8, and 9.1.5.	08
	Sections 1.3, 2.2, 3.1.1, 3.1.5, 3.16, 3.2, 3.3, 4.1.2, 4.2, 4.3.2, 4.4, 4.9.1.1, 4.9.3, 4.10.2, 4.10.3, 4.12.2, 5, 6, 7.1, 7.2.1, 8, 9	09

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)

1.3.1.1 Three-level CA Hierarchy

The TunTrust PKI consists in a three-level CA hierarchy; the top level is the **Tunisian National Root CA**, the highest level of authority managed by TunTrust. The TunTrust PKI is formed using additional subordinates and issuing CAs as depicted in figure 1.

The TunTrust PKI consists of the following CAs:

- One ***Tunisian National Root CA*** root-signing all TunTrust subordinate CAs and kept offline.
- One subordinate CA ***Tunisia GOV CA****:* This SubCA is signed by the ***Tunisian National Root CA*** *and* is *responsible of* the issuance of the Issuing Certification Authorities.
- Two Issuing CAs :
    - ***TnTrust GOV CA*** issued by ***Tunisia GOV CA*** and operates online to issue SSL certificates.
    - ***TnTrust Qualified GOV*** issued by ***Tunisia GOV CA*** and operates online to issue Qualified certificates.

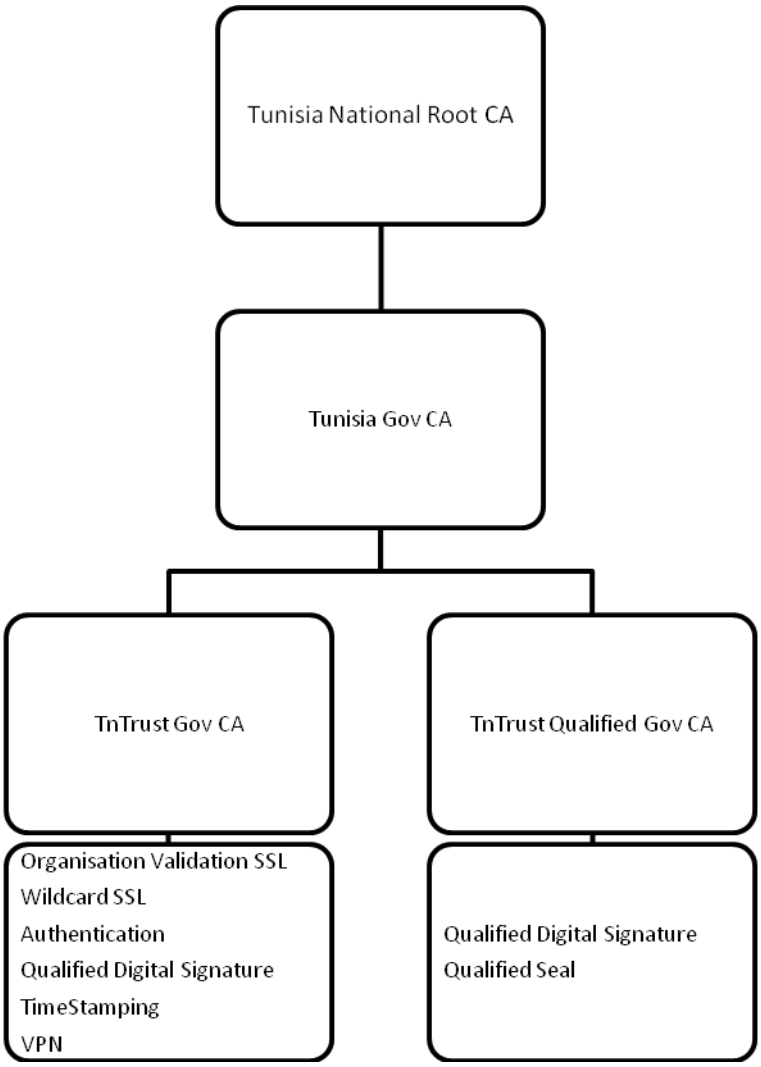

Fig-1: TunTrust CAs Hierarchy

- The OID of TunTrust is joint-iso-itu-t(2) country(16) tn(788) public-sector(1) public-sector-enterprises(2) ANCE(6).
- The issuing CA "**TnTrust Gov CA**" is under Policy OID: 2.16.788.1.2.6.1.9.
- *The issuing CA "**TnTrust Qualified Gov CA**" is under Policy OID: 2.16.788.1.2.6.1.10.*

TunTrust issues certificates containing the following OID arcs:

a) End User Certificates issued by **TnTrust Gov CA**:

Service	Description	OID
TimeStamping	A Certificate to issue timestamp tokens	NCP+ OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.9.1.7

b) End User Certificates issued by **TnTrust Qualified Gov CA**:

Service	Description	OID
ID-Trust	An authentication and digital signing Certificate on a QSCD for natural person, that is compliant to ETSI EN 319 411-2.	QCP-n-QSCD OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.1
ID-Trust Pro	An authentication and digital signing Certificate on a QSCD for natural person with professional attributes, that is compliant to ETSI EN 319 411-2.	QCP-n-QSCD OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.1
DigiGO	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: 2.16.788.1.2.6.1.10.1.3
DigiGO Pro	An authentication and digital signing Certificate on a remote QSCD for natural person with professional attributes, that is compliant to ETSI EN 319 411-2.	QCP-n-QSCD OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.3
Enterprise-ID	Qualified certificates for electronic seal (eSeal) issued to legal persons or public authorities, that is compliant to ETSI EN 319 411-1.	QCP-l-QSCD OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.2

1.3.2 REGISTRATION AUTHORITY (RA)

TunTrust CAs rely on a dedicated network of registration authorities made of :

- a Central Registration Authority (CRA) operated by TunTrust, and
- a set of Delegated Registration Authorities (DRAs) composed of one or several Physical Verification Point (PVP) and/or a Video Verification Service (VVS).

TunTrust has a contractual agreement with Delegated Third Parties which indicates the authorization for their role as DRAs 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:

- Identifying and authenticating Applicants for Certificates,
- Accepting, evaluating, approving or rejecting the registration of Certificate applications,
- Registering Subscribers for certification services,
- 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 files (electronic and / or paper).

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 Authorities (DRAs) that have to abide by all the requirements of the DRA agreement and this CP/CPS. DRAs may, however implement more restrictive practices based on their internal requirements.

The Delegated Registration Authorities (DRAs) aim to operate one or several PVPs and VVSs and proceed, under strictly determined and controlled conditions, to the validation of an Applicant's identity through:

- physical face-to-face identification,

  or

- video identification that provide equivalent assurance in terms of reliability to the physical presence.

Any DRA can delegate, in the Physical Verification Points (PVPs) or the Video Verification Services (VVSs), the Applicant's identity verification function and the receipt of documentation and, if applicable, the compiling of documentation and verification of its suitability as well as the delivery of the cryptographic device.

Based on the documentation collected by the PVP or the VVS, the DRA operator checks the documentation and, if applicable TunTrust CA issues the certificate with no need to carry out a new identity verification.

1.3.2.3 Physical Verification Point (PVP)

A Point of Physical Verification always depends on a DRA. The physical authentication process must comply to this CP/CPS.

The main mission of Physical Verification Points (PVP) is to :

- collect Applicant personal data including full name, date and place of birth, email address, mobile phone number;
- provide evidence of the applicant’s physical presence;
- and deliver the documentation to the DRA where all certificate requests are collected and securely transmitted to CRA.

The PVPs' functions include compiling the documentation submitted, checking its suitability for the type of certificate requested and delivery to the applicant in the case of the cryptographic support (smart card/token).

PVPs do not have registration powers; they are contractually bound to a DRA. With regards to registration, PVPs have direct contact with the Subscribers and must have direct contact with the DRA, but have no direct contacts with the CRA nor the CA.

An official list of Physical Verification Points is available on TunTrust website under the following URL: https://www.tuntrust.tn/fr/content/ou-obtenir-mon-certificat

1.3.2.4 Video Verification Service (VVS)

A Video Verification Service may be provided by a DRA in order to remotely authenticate the physical identity of a person. The Video authentication process must comply to this CP/CPS and to remote identification requirements set in the RA Agreement.

The main mission of a Video Verification Service is to:

- collect Applicant personal data including full name, date and place of birth, email address, mobile phone number;
- make a digital copy of Applicant identification document (passport, identity card or residence permit).
- confirm subject personal data in a live video to complete identification materials and aimed to avoid identification fraud.

The collected data are sent, by the VVS operator, to CRA Servers where they are securely stored.

1.3.3 SUBSCRIBERS

Subscribers are either Legal Entities or 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 both the Subject of the Certificate and the entity that contracted with TunTrust CA for the Certificate's issuance. 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.

Subscribers of end entity Certificates issued by TunTrust CA include employees and agents involved in day-to-day activities within TunTrust CA that require access to TunTrust CA network resources. Subscribers are also sometimes operational or legal owners of signature creation devices that are issued for the purpose of generating a Key Pair and storing a Certificate.

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 Sections 1.3.2, 1.3.3 and 1.3.4, TunTrust will involve other parties as needed. TunTrust will contractually obligate each party to comply with all applicable requirements in this CP/CPS and monitor its compliance.

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 and TunTrust Time Stamping Policies.
- 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.

Requests for information as well as any other inquiry associated with this CP/CPS should be addressed to:

TUNTRUST - Agence Nationale de Certification Electronique
Technopark El Ghazala,
Road of Raoued,
Ariana, 2083
Tunisia.

Tel.: +216 70 834 600
Mail: pki@tuntrust.tn
Web: https://www.tuntrust.tn

1.5.2 Contact person

The contact person, designated by the Board of Directors of TunTrust, is a member of the Board of Directors of TunTrust. See section 1.5.1 for contact details .

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 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 below 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 these Requirements.

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until

encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Authorized Ports: One of the following ports: 80 (http), 443 (http), 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 6844 (http:tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate misissue."

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 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 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.

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

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

DNS TXT Record Phone Contact: The phone number defined in section B.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 contract (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 Name: The label 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 assigns). Effective Date: 1 July 2012.

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 labels of all superior nodes in the Internet Domain Name System.

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.

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 label 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, 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. 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.

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.

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.

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.

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 found in this document.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved:

http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

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

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.

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.

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: A Certificate with a maximum validity period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID (2.23.140.2.1), or (ii) is issued under a CA where there are no certificate paths/chains to a root certificate subject to these 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 Specialists: Someone who performs the information verification duties specified by these Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

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 an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Wildcard Domain Name: A Domain Name consisting of a single asterisk character followed by a single full stop character (“*.”) followed by a Fully-Qualified Domain Name.

1.6.2 ACRONYMS

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CAA	Certification Authority Authorization

ccTLD	Country Code Top-Level Domain
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
VVS	Video Verification Service

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 (e.g: 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 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. 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 to Relying Parties.

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 the naming and profile document (published in the repository http://www.tuntrust.tn/repository).

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

TunTrust uses distinguished names (DN) that identify both the subject and issuer of the certificate. The subject and issuer name contained in a certificate must be meaningful in the sense that TunTrust has proper evidence of the existing association between these names and the entities to which they belong. To achieve this goal, the use of a name must be authorized by the rightful owner or a legal representative of the rightful owner.

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

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

3.1.5 UNIQUENESS OF NAMES

The full combination of the Subject Attributes (Distinguished Name) has to be unique and shall conform to all applicable X.500 standards for the uniqueness of names.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

TunTrust will issue certificates including trademarks only if the trademark is registered in the Tunisian National register of Enterprises which is called "Registre National des Entreprises" (or the foreign equivalent for foreign companies registered under foreign law). TunTrust will not issue certificates with trademarks that are not documented in the National Register of Enterprises (or the foreign equivalent for foreign companies registered under foreign law).

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

TunTrust uses various circuits for issuing certificates in which the private key is managed **DIFFERENTLY. EITHER THE** Subscriber **OR** TunTrust **CAN CREATE THE PRIVATE KEY** as described in the table below:

Type of Certificate	Private Keys generation
ID-Trust, ID-Trust Pro, Enterprise-ID on cryptographic token (QSCD)	Key generation is performed under TunTrust's direct control, Private Keys are generated directly on compliant Qualified Electronic Signature Creation Devices (QSCD). Certificate enrollment requests are sent via the QSCD middleware to the Token Management System that transmits the request to the issuing CAs as signed and encrypted messages over a HTTPS link.
DigiGO,	• Private Keys are generated and stored under the control of the Subscriber on a

Enterprise-ID on HSM (QSCD)	Hardware Security Module (HSM) that is located in TunTrust data center. Access by the Subscriber to the keys is protected using multifactor authentication aimed to achieve the same level of assurance of sole control as achieved by a cryptographic token ; or • Private Keys are generated and stored under the control of the Subscriber on a Hardware Security Module that is located in the Subscriber's data center. The generation of private keys in the Subscriber's HSM is witnessed by a TunTrust trusted agent.

3.2.2 AUTHENTICATION OF ORGANIZATION AND DOMAIN IDENTITY

TunTrust verifies the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of Section 3.2.2.1. TunTrust inspects any document relied upon for alteration or falsification.

3.2.2.1 IDENTITY

The following official documents are required for the verification of the organizational existence and identity of Applicants and/or to validate the relationship of a physical person with a legal person:

a) Constitutive act, or recent extract from the National Register of Enterprises not older than 03 months (or the foreign equivalent for foreign companies registered under foreign law) including at least the company name, legal address, tax identification number, first name and last name of the legal representative. The identity and head office address of government entities requesting certificate is verified based on the legal documents and official correspondences with the requesting agency or a superior governing governmental agency.

b) A copy of the identity evidence (identity card, passport or Tunisia residency card) of one of the physical persons who is a legal representative of the legal person. For Government entities, the identity of the legal representative is established by legal documents and by referring to subsequent government gazette or other QGIS.

c) In case the relationship of a physical person with a legal person is to be validated and certified in the Certificate, the person identified in (b) shall sign the appropriate guarantee as provided in the applicable Certificate application form.

d) The authority of the Applicant to request a Certificate on behalf of the organization must be verified in accordance with Section 3.2.5.

3.2.2.2 DBA/TRADENAME

If the Subject Identity Information is to include a DBA or tradename, TunTrust verifies the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition (such as a Constitutive act, or recent extract from

the national register of companies not older than 3 months or the foreign equivalent for foreign companies registered under foreign law);

2. Communication with a government agency responsible for the management of such DBAs or tradenames.

3.2.2.3 VERIFICATION OF COUNTRY

TunTrust verifies the country associated with the Subject as specified in Section 3.2.2.1.

3.2.2.4 VALIDATION OF DOMAIN AUTHORIZATION OR CONTROL

TunTrust does not issue SSL certificates from the ***TnTrust Qualified Gov CA***.

3.2.2.5 AUTHENTICATION FOR AN IP ADDRESS

TunTrust does not issue certificates with IP addresses.

3.2.2.6 WILDCARD DOMAIN VALIDATION

TunTrust does not issue SSL certificates using ***TnTrust Qualified Gov CA***.

3.2.2.7 DATA SOURCE ACCURACY

TunTrust maintains a list of accepted data sources that consider the following:

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.

Information are checked manually and/or automatically through administrative authorities services to ensure the accuracy of information.

3.2.2.8 CAA RECORDS

TunTrust does not issue SSL certificates using ***TnTrust Qualified Gov CA***.

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 one of these processes: certificate application, certificate issuance, subject device provisioning.

An identity validation of an individual Subscriber (or Subject if it differs from the Subscriber) for issuance of a certificate, includes the following:

- The Subscriber must be physically present in front of a TunTrust (CRAO) or (PVPO) during registration process or use a Video Verification Service which provides equivalent assurance to physical presence.
- The Subscriber must provide for verification a valid and authentic ID photo (including national identity card, passport or residence permit),

- TunTrust RA verifies the authenticity and validity of the provided identity proof according to this CP/CPS.

Identification and authentication requirements for an individual aiming to have its professional attributes certified must provide evidence of the applicability of such professional attributes. When these professional attributes are related to an organization, the individual must comply with the provision stated in section 3.2.2 of the CP/CPS.

3.2.3.1 VALIDATION OF SUBSCRIBER EMAIL

TunTrust takes reasonable measures to verify that the Applicant submitting the request controls the email account referenced in the Certificate, or has a legal right to request a Certificate including the email address. TunTrust systems perform a challenge-response procedure by sending an email to the email address to be included in the Certificate. The Applicant must respond with a shared secret within a limited time to demonstrate that they have control over that email address.

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 possession 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 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. TunTrust may also verify that the applicant has control over the mobile phone number by requesting a copy of the mobile phone contract or by direct communication with the telecom operators when possible.

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

ID-Trust DigiGO	**For natural person with no professional attributes :** Face-to-face identification through physical presence or through suitable video identification is mandatory to validate the personal credentials of the Applicant together with verification that the Applicant has control over the email address to be listed within the Certificate as detailed in section 3.2.4. For DigiGO Certificates, TunTrust verifies that the Applicant has control over the mobile phone number used to activate the Applicant private keys stored in the remote QSCD as detailed in section 3.2.4

ID-Trust Pro DigiGO Pro	**For natural person with professional attributes :** The certificate application form is signed and stamped by the legal representative of the entity and signed by the Applicant and each of them must provide a copy of his or her ID. The full name of the legal representative must be recorded in the Register Trade extract of the organization Face-to-face identification through physical presence or through suitable video identification is mandatory to validate the personal credentials of the Applicant together with verification that the Applicant has control over the email address to be listed within the Certificate as detailed in section 3.2.4 For DigiGO Pro Certificates, TunTrust verifies that the Applicant has control over the mobile phone number used to activate the Applicant private keys stored in the remote QSCD as detailed in section 3.2.4
Enterprise-ID	**For legal person:** The certificate application form is signed and stamped by the legal representative of the entity and signed by the Applicant and each of them must provide a copy of his or her ID. The full name of the legal representative must be recorded in the Register Trade extract of the organization Personal appearance of Applicant is mandatory before a suitable Registration Authority to validate the personal credentials of the Applicant together with verification that the Applicant has control over the email address to be listed within the Certificate as detailed in section 3.2.4

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. Examples of reasons for revocation include a breach of the Subscriber Agreement, non-payment of applicable fees or not retrieving a certificate within 90 calendar days from the generation date of the certificate.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

TunTrust maintains its own blacklists of individuals from whom and entities from which it will not accept Certificate applications. In addition, other external sources such as government denied lists or internationally recognized denied persons lists which are applicable to the jurisdictions in which TunTrust operates are used to screen out unwanted Applicants.

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 RA.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

The issuance of Certificates by TunTrust CAs will be pursuant to forms and documentation required by TunTrust. Notwithstanding the foregoing, the following steps are required in any application for a Certificate: (i) Identity of the Applicant is to be established in accordance with section 3.2 of this CP/CPS, (ii) a Key Pair for the Certificate is to be generated in a secure environment, (iii) the binding of the Key Pair to the Certificate shall occur as set forth in this CP/CPS, and (iv) TunTrust CA shall enter into contractual relations with the Applicant for the use of that Certificate.

For provision of services, TunTrust operates a Central Registration Authority connected to a network of registration authorities including DRA(s) 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.

When face-to-face identification is required, Applicant may present himself, in person, to the CRA or one of the PVPs bringing with him/her the documents required by the applicable CP/CPS. A CRA / PVP officer will perform a face-to-face initial identification of an individual Applicant (or Subject if it differs from the Subscriber) for issuance of a certificate as described in Section 3.2.2.

Face-to-face identification may also be performed remotely through Video Verification Services provided by DRA. The Video Verification process must comply to the CP/CPS and to the requirements set in the RA Agreement in order to be consider as equivalent to the physical face-to-face identification.

Based on the documentation collected by the PVP or the VVS, the DRA operator checks the documentation and, if applicable TunTrust CA issues the certificate with no need to carry out a new identity verification.

4.2 Certificate Application Processing

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

Certificate type	Enrollment process
ID-Trust	• Face-to-face identification of Applicant either through physical presence or remote video identification. Applicant must provide :

DigiGO	– Order Form signed by Applicant; – Copy of ID photo (identity card, passport or residence permit) • The following verification tasks are performed by TunTrust RAs: – Identity of Applicant as specified in Section 3.2.3 – Order Form is duly filled in and signed by the Applicant – Applicant has been informed of and accepted the conditions and terms of use of the Certificate. – Control of email address to be listed within the Certificate through a challenge response mechanism. Application is not processed until successful challenge-response verification of email address. • Upon successful verification of Certificate Application , the RA operator initiates a certificate signing request using multi-factor authentication.
ID-Trust Pro and DigiGO Pro	• Face-to-face identification of Applicant either through physical presence or remote video identification. • Application must include the following items : – Order Form containing The “Subscriber Part” duly completed and signed by Applicant, and the “Subscriber Organization Part” duly filled in and signed by a legal representative (or his/her duly appointed delegate) of the organization to which the Subscriber belongs. – Constitutive act, or recent extract of the National Register of Enterprises not older than 03 months (or the foreign equivalent for foreign companies registered under foreign law) including at least the company name, legal address, tax identification number, first name and last name of the legal representative who signed the “Subscriber Organization Part” of the Order form . – Copy of national ID photo of Applicant (identity card, passport or Tunisia residency card) • The following verification tasks are performed by TunTrust RAs: – Identity of Applicant and legal representative as specified in Section 3.2.3 – Order Form is duly filled in and signed by the Applicant and the legal representative. – Identity of the Organization as specified in Section 3.2.2 – Applicant affiliation with the organization and that the Applicant has the authority to possess a Certificate indicating the affiliation as described in section 3.2.2. – Applicant has been informed of and accepted the conditions and terms of use of the Certificate.

	– Control of email address to be listed within the Certificate through a challenge response mechanism. Application is not processed until successful challenge-response verification of email address. – For DigiGo Certificate, control of Mobile Phone Number used as a authentication factor is verified through a challenge response mechanism. DigiGO Application is not processed until successful challenge-response verification of mobile phone number. a) Upon successful verification of Certificate Application , the RA operator initiates a certificate signing request through using multi-factor authentication.
Enterprise ID	• Applications for Enterprise-ID shall be submitted by the legal representative of the Applicant. • Enterprise-ID Certificate application includes the following: – Order Form duly completed and signed by the contract signer and the legal representative or its duly mandated Certificate Manager. – Constitutive act, or recent extract of the National Register of Enterprises not older than 03 months including at least the company name, legal address, tax identification number, first name and last name of the legal representative. – Copy of ID photo of Contract Signer (identity card, passport or Tunisia residency card) – Copy of ID photo of legal representative or Certificate Manager (identity card, passport or Tunisia residency card) • The following verification tasks are performed by TunTrust RAs: – Validation of the identity of the organization (section 3.2.2) : Organization must be a public or private entity under the Tunisian Jurisdiction – Validation of the identity of the signatories of the request (section 3.2.3); • Assurance that Signatories have been informed of and accepted the conditions and terms of use of the Certificate.

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, 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.

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

Upon receipt of an approved Certificate signing request, TunTrust Issuing CAs will verify the authorization, compliance, completeness of such a request.

Upon successful verification, the Issuing CA will then issue the requested Certificate.
Certificate issuance by the Root CA SHALL require an individual in a trusted role and authorized by TunTrust to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

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 email address that was supplied by the Subscriber during the enrollment process and will be provided with appropriate instructions on how to obtain the certificate. If the certificate is presented to the subscriber immediately, special notification may not be necessary.

The Subscriber (or his representative) must retrieve its Certificate on the cryptographic token within a period of time not exceeding 90 calendar days starting from the date of notification of the issuance of the Certificate.

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 or the reliance upon a Certificate signifies acceptance by that person of the terms and conditions 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.

TunTrust CA shall inform the Subscriber to validate that the details present in the certificate match his or her requirements. 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.

However, if the Subscriber (or his representative) did not present himself to retrieve his ID-Trust certificate (digital signature certificate) from TunTrust CRA or any PVP within 90 calendar days from the date of notification of issuance of this certificate, TunTrust reserves the right to revoke this certificate without any prior notice. The Subscriber whose certificate has been revoked under these conditions, can file a new certificate request at no additional cost using an invoice provided by TunTrust.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

Refer to Section 2.1.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

DRAs may receive notification of a Certificate's issuance if the DRA was involved in the issuance process.

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.

At the end of the useful life of a Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup.

4.5.2 Relying Party Public Key and Certificate Usage

Within this CP/CPS, 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.

Authorized 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

Not Applicable. TunTrust does not support re-key.

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

4.7.1.1 RE-KEY OF DEVICE CERTIFICATES

Not Applicable. TunTrust does not support re-key.

4.7.1.2 RE-KEY OF END-USER CERTIFICATE

Not Applicable. TunTrust does not support re-key.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

Not Applicable. TunTrust does not support re-key.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUEST

Not Applicable. TunTrust does not support re-key.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable. TunTrust does not support re-key.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Not Applicable. TunTrust does not support re-key.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

Not Applicable. TunTrust does not support re-key.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable. TunTrust does not support re-key.

4.8 Certificate Modification

Certificate modification is the process through which a Subscriber requests a Certificate with modified subject information. TunTrust shall deem 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:

a) The Subscriber requests in writing that TunTrust revoke the Certificate;
b) The Subscriber notifies TunTrust that the original Certificate request was not authorized and does not retroactively grant authorization;
c) TunTrust obtains evidence that the Subscriber'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 and 6.1.6; or
d) TunTrust obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

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

e) The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
f) TunTrust obtains evidence that the Certificate was misused;

g) TunTrust is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
h) TunTrust is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
i) TunTrust is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
j) TunTrust is made aware of a material change in the information contained in the Certificate;
k) TunTrust is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
l) TunTrust determines or is made aware that any of the information appearing in the Certificate is inaccurate;
m) TunTrust'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
n) Revocation is required by this CP/CPS.

.

TunTrust revokes a Certificate if the Subscriber (or his representative) did not present himself to retrieve his/her ID-Trust certificate (digital signature certificate) from TunTrust CRA or any PVP within 90 calendar days from the date of notification of issuance of this certificate. In this case, TunTrust reserves the right to revoke this certificate without any prior notice and the Subscriber whose certificate has been revoked under these conditions, can file a new certificate request at no additional cost with an invoice provided by TunTrust.

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 and 6.1.6,
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 shall accept authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or its appropriately authorized Contract Signer. 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 Section 1.5.2. 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:

- Using TunTrust online service available at https://www.tuntrust.tn/fr/content/revocation-certificat. In this case, the Subscriber is required to provide a challenge (that was communicated to the Subscriber upon delivery of the certificate) and the Common Name listed in the certificate. The Subscriber is also requested to provide an email address to which a notification will be sent once the certificate is revoked.
- Physical presence before a TunTrust CRA operator: Either the contract signer or the legal representative of the Subscriber must be physically present at the headquarters (Section 1.5.2) of TunTrust and request the revocation of a Certificate in writing after providing a valid ID.
- For DigiGO certificates, the Subscriber may revoke his/her Certificate by logging in to his/her personal space at https://digigo.tuntrust.tn .

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 sections 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 Section 4.9.1.1.

The date selected by TunTrust considers the following criteria:

a) The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
b) The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
c) The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
d) The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
a) Relevant legislation.

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 RFC6960 and/or RFC5019. OCSP responses are signed by an OCSP Responder whose Certificate is signed by the 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

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

For the status of Subscriber Certificates:

- TunTrust updates information provided via an OCSP at least every four days. OCSP responses from this service will not exceed an expiration time of ten days.

For the status of Subordinate CA Certificates:

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

OCSP Responders that receive a request for status of a Certificate that has not been issued, do not respond with a "good" status for such Certificates.

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.

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 ten 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 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 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.

TunTrust does not store copies of subscriber private keys; Subscriber's key back-up, escrow and key recovery are not possible.

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 the CA by law.

f) The Certificate Management Process includes:

g) physical security and environmental controls;

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

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

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

k) 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 takes into account 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 sites its operations within secure data centers located in Tunisia exhibiting the following features:

- Protected by physical barriers, including solid walls that extend from real floor to real ceiling to prevent unauthorized entry to TunTrust certificate manufacturing facilities,
- 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

TunTrust protects its equipment from unauthorized access and implements physical controls to reduce the risk of equipment tampering. 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.

The buildings housing TunTrust's CA and TSA systems have security personnel on duty full time (24 hours per day, 365 days per year). The exterior and internal passageways of the buildings are under constant video surveillance. TunTrust securely stores all removable media and paper containing sensitive plain-text information related to its CA operations in secure containers in accordance with its Data Classification Procedure.

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

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

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. 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 and fire.

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 performs routine backups of critical system data, and other sensitive information. The backed up data are stored in physically 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, document control, processes relating to Subscriber Certificate registration, generation and revocation. They are also responsible for interacting with Applicants and Subscribers, managing the Certificate request queue and completing the Certificate approval checklist as identity vetting items are successfully completed. 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, ...). 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 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.

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, other than the Auditor role. 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 8

(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

1. 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

Prior to the engagement of any person, whether as an employee, agent, or an independent contractor, TunTrust verifies the identity and trustworthiness of such person. TunTrust employs a sufficient number of personnel that possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function.

TunTrust personnel fulfill the requirement through expert knowledge, experience and qualifications with formal training and education, actual experience, or a combination of the two. 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 in trusted roles are free from conflict of interests that might prejudice the impartiality of the CA operations. TunTrust does not appoint to a trusted role any person who is known to have a conviction for a serious crime or another offence if such conviction affects his/her suitability for the position.
Personnel do not have access to the trusted functions until any necessary checks are completed and results analyzed. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation where permitted by law.

Any use of information revealed by background checks by TunTrust shall be in compliance with applicable laws in Tunisia.

5.3.3 Training requirements

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 the CA's 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 the organization, or by request of an individual employee.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

Appropriate disciplinary sanctions are applied to personnel violating provisions and policies within the applicable CP/CPS or CA related operational procedures.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

TunTrust does not involve Delegated Third Party's personnel in the issuance of a Certificate.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

TunTrust makes available to its personnel this CP/CPS. 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 each Delegated Third Party record details of the 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.

1. CA key lifecycle management events, including:
   a. Key generation, backup, storage, recovery, archival, and destruction; and
   b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
   a. Certificate requests and renewal requests, and revocation;
   b. All verification activities stipulated in this CP/CPS;
   c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
   d. Acceptance and rejection of certificate requests;
   e. Issuance of Certificates; and
   f. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
   a. Successful and unsuccessful PKI system access attempts;
   b. PKI and security system actions performed;

c. Security profile changes;

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

e. Firewall and router activities; and

f. Entries to and exits from the CA facility.

Log entries include the following elements:

1. Date and time of entry;
2. Identity of the person making the journal entry; and
3. Description of the entry.

5.4.2 Frequency of processing and archiving Audit logs

Log events deemed to be security sensitive will automatically generate security incident reports. A human review of the logging processes is also performed on application and system logs at least once every 30 days to validate the integrity of logging processes and ensure that monitoring, logging, alerting, and log integrity-verification functions are operating properly.

5.4.3 Retention Period for Audit Log

TunTrust retains any audit logs generated for at least seven years. 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 facilities and in an off-site location. The events are logged in a way that they cannot be deleted or destroyed for any period of time that they are retained.

The records of events are protected to prevent alteration and detect tampering and to ensure that only trusted individuals with authorized access are able to perform any operations without modifying integrity, authenticity and confidentiality of the data.

5.4.5 Audit Log Backup Procedures

Audit logs are backed-up in a secure location, under the control of an authorized trusted role, and separated from their component source generation. 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. Manually generated audit data is recorded by TunTrust personnel.

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 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.

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.

5.5 Records archival

5.5.1 Types of records archived

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,
- TunTrust CAs keys generation and destruction.

5.5.2 Retention period for archive

TunTrust retains all documentation relating to certificate applications and the verification thereof, and all Certificates and revocation thereof, for at least 20 years after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of archive

Physical and logical access controls are in place to prevent unauthorized access to archived data. 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 (two years prior to its expiration) and uses the old Private Key only to sign CRLs. A new CA signing key pair is commissioned and all subsequently issued certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

5.7 Compromise and disaster recovery

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

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 the 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.

If TunTrust determines that its computing resources, software, or data operations have been compromised, TunTrust will investigate the extent of the compromise and the risk presented to affected parties. Depending on 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 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. The Disaster Recovery Plan is regularly tested, verified and updated to be operational in the event of a disaster. The TunTrust operation is designed to restore the services detailed in Section 2.1within six (6) hours of main site system failure.

In the event that the disaster is such that the availability can no longer be met, TunTrust must make all reasonable efforts to notify any Relying Parties of the disruption of service.

5.8 CA or RA Termination

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

- Notice period without seeking Subscriber's consent
- Revoke all certificates that are still un-revoked or un-expired as specified in the notice and publish final CRLs,
- Destroy all private keys.
- Make reasonable arrangements to preserve its records according to the applicable CP/CPS.
- Reserve its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as TunTrust is.

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

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 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 keys in a physically secured environment as described in this CP/CPS;
2. generates the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. generates the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in section 6.2.1 of this CP/CPS;
4. logs its CA key generation activities; and
5. maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CP/CPS and (if applicable) 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 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 and remote electronic seal are generated in a 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,
- May be sent to the Subscribers (identified person) shipping address after registration at back-office.

- May be distributed to the Subscriber in a face-to-face process once identified and authenticated by the CRAO/PVPO in accordance with the applicable CP/CPS,
- Is distributed using a channel that is separated from the one used for distribution of Subscriber's Private Key Activation Data.

When Subscriber key pairs are generated on a remote QSCD by the Subscriber, private key delivery to the Subscriber is performed inside the remote QSCD.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

In the case of ID-Trust and Enterprise-ID certificate, the Subscriber certificate:

- Is generated securely within the TunTrust QSCD,
- Has its corresponding Public Key certified by the CA,
- May be sent to the Subscribers (identified person) shipping address after registration at back-office.
- May be distributed to the Subscriber in a face-to-face process once identified and authenticated by a TunTrust authorized CRAO in accordance with the applicable CP/CPS,
- Is distributed using a channel that is separated from the one used for distribution of Subscriber's Private Key Activation Data.

In the case of certificates for remote electronic signature and certificates for remote electronic seal ,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 or electronic seal.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

TunTrust provides its Public Keys to Relying Parties as trust anchors in commercial browsers and operating system root stores. Commercial web browsers and platform operators are encouraged to embed Root Certificate Public Keys into their root stores and operating systems. Issuing CA Public Keys are delivered to the Subscriber in the form of a chain of Certificates or via a Repository operated by TunTrust and referenced within the profile of the issued Certificate through AIA (Authority Information Access) extension.

6.1.5 KEY SIZES

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

Root CA Certificate:

	Value
Digest algorithm	SHA-256
RSA modulus size (bits)	4096

Intermediate CA Certificates:

	Value
Digest algorithm	SHA-256
RSA modulus size (bits)	4096

Issuing CA Certificates:

	Value
Digest algorithm	SHA-256
RSA modulus size (bits)	3072

Subscriber certificates:

	Value
Digest algorithm	SHA-256
RSA modulus size (bits)	2048

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

TunTrust generates Key Pairs in accordance with FIPS 186-2. The value of the public exponent is equal to : 65537.

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

The use of a specific key is determined by the key usage extension in the X.509 Certificate. TunTrust sets key usage of Certificates depending on their proposed field of application via the v3 Key Usage Field for X.509 v3 (see Section 7.1).
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; and
- Certificates for Subordinate CAs and Cross Certificates.

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.

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 or EAL4+ requirements.
- Issuing CAs keys: The HSM used for CA keys meets FIPS 140-2 level 3 or EAL4+ requirements.
- Subscriber keys:
    -
    - ID-Trust and Enterprise-ID Certificates: TunTrust uses a hardware cryptographic device (USB-key cryptographic token or smart card) where the subscriber keys are generated and stored. This hardware for key pair generation and private key storage of end-user Subscribers is, at a minimum, rated at FIPS 140-2 Level 3.
    - DigiGO Certificates : The HSM used for Remote signing and Remote electronic seal keys meets FIPS 140-2 level 3 or 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.
- Intermediate CA keys : Intermediate 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 8).
- Subscriber keys on local QSCD: The subscriber has single-person control of the subscriber keys.
- 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 + Password + 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.

In case of a local QSCD (cryptographic token), the Subscriber Private Keys cannot be extracted or restored from the QSCD and are not backed up.

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.

If TunTrust becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then TunTrust will revoke all certificates that include the Public Key corresponding to the communicated Private Key.

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).
- Intermediate CAs keys: The intermediate CAs keys are activated with two user key (physical) and two user PIN (knowledge).
- Issuing CA keys: The Issuing CA keys are activated with two user key (physical) and two user PIN (knowledge).
- Subscriber keys on local QSCD: The subscriber private key is activated with a hardware cryptographic device PIN or only a user PIN (knowledge).
- Subscriber Private Keys on Remote QSCD : The Subscriber private key is protected by username, password 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 prevents unauthorized access to any activated cryptographic modules. 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 Tunisian National Root CA is valid for 20 years and 06 months.
- The intermediate CAs are valid for 15 years and 03 months.
- The issuing CAs certificates are valid for 10 years and 01 month.
- The end-user certificates can have a lifetime of 1 or 2 years.

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.
For Certificates on local QSCD, TunTrust will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated local QSCD.

Activation data used (username, password and OTP code) to protect Remote QSCD containing Subject's private keys are generated in accordance with the compliance requirements of the QSCD.
All TunTrust personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. TunTrust employees are required to create non-dictionary, alphanumeric passwords with a minimum length and to change their passwords on a regular basis.

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 CAs activation data is stored on smart cards.

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

The Subscriber shall memorize the activation credentials (PIN, PUK, username, password, OTP) and not share them with anyone else.

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 controls ensure the security of TunTrust operated computer systems:

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

TunTrust enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.

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. Any changes in the configuration of TunTrust CA systems trigger alerts automatically and in real time.

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.

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 and Subscriber certificates are described in the Naming and Profiles Document available at https://www.tuntrust.tn/repository.

7.1.1 VERSION NUMBER(S)

TunTrust CAs issue X.509 version 3 certificates.

7.1.2 CERTIFICATE EXTENSIONS

X.509 v3 extensions are supported and used as indicated in the Certificates profiles as described in the Naming and Profiles Document available at https://www.tuntrust.tn/repository.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

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

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.

7.1.4.1 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.

7.1.5 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

Tunisian National Root CA certificates 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 (as also described in the Naming and Profiles Document available at https://www.tuntrust.tn/repository).

7.1.6.4 SUBSCRIBER CERTIFICATES

The certificate policy identifiers of the Subscriber Certificates are listed in the Naming and Profiles Document available at https://www.tuntrust.tn/repository.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

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

TunTrust CA follows Section 7.1.6 of CA/B Forum Baseline Requirements.

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)

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

7.2.2 CRL AND CRL ENTRY EXTENSIONS

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

TunTrust CRL profiles description is available as in the naming and profile (published in repository https://www.tuntrust.tn/repository).

7.3 OCSP profile

The TunTrust OCSP functionality is built according to RFC 6960.

The 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.

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 as in the naming and profile (published in repository https://www.tuntrust.tn/repository).

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

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 requirements of the then-current ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 421 and CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (latest relevant version).

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 by the CA/Browser Forum.

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 the audited party or is a result of unsatisfactory results of a previous audit.

Material exceptions or deficiencies identified during an audit will result in a determination of actions to be taken. This determination is made by the independent auditor with input from the TunTrust management. TunTrust management is responsible for developing and implementing a corrective action plan.

8.2 Identity/qualifications of assessor

The 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 Froum 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 shall utilize 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 WebTrust for CAs and WebTrust for CAs SSL Baseline with Network Security. 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 Section 8.2.

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 management with input from the auditor. If exceptions or deficiencies are identified, TunTrust management is responsible for developing and implementing a corrective action plan. If TunTrust determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the PKI, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, TunTrust management will evaluate the significance of such issues and determine the appropriate course of action.

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. Such parties include the Common CA Database.

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 charges fees for issuing and renewal of certificates according to the respective price list published on its website https://www.tuntrust.tn or made available upon request.

The update of the fees goes through the Board of Directors of TunTrust. After a favorable opinion, TunTrust forwards the proposal to the Ministry of Information Technology of Tunisia for approval.

9.1.2 Certificate access fees

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

9.1.3 Revocation or status information accessfees

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 charge for other additional services such as time stamping.

9.1.5 Refund Policy

TunTrust does not refund the fees of certificates except for when an ID-Trust certificate of a subscriber who did not retrieve his/her certificate within 90 calendar days from the date of notification of the issuance of the said certificate, was revoked. In the latter case, an invoice is provided to the subscriber in order to submit a new certificate application with no additional fees

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

Insurance coverage is described in Section 9.2.1. 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

The following items are classified as being confidential information and therefore are subject to reasonable care and attention by TunTrust personnel including validation specialists and administrators:

- Personal Information as detailed in Section 9.4;
- Audit logs from CA and RA systems;
- Activation data used to active CA Private Keys as detailed in Section 6.4;
- Internal TunTrust business process documentation including Disaster Recovery Plan (DRP) and Business Continuity Procedures (BCP); and
- Audit Reports from an independent auditor as detailed in Section 8.

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° 2004-63of 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 or CRL 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.

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 retains ownership of Certificates; however, it 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:

1. The Subscriber that is a party to the Subscriber Agreement
2. 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
3. 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 iths 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 and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (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 (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (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 subject:organizationalUnitName attribute would be misleading; (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 Sections 3.2 and 11.2; (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** : That 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 RA represents that:

1. Information provided by the RA does not contain any false or misleading information,
2. Translations performed by the RA are an accurate translation of the original information, and
3. All Certificates requested by the RA 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 install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and 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 TunTrust discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

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 indicia 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 section 9.15.5. 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

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.

9.10 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 commercially reasonable methods to communicate with each other.

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 or other products and services. 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 SHALL 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, MUST be 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.