Tunisian National PKI

Certificate Policy / Certificate Practice Statement

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

	Author	Validated by	Approved by
Entity :	TunTrust	Steering comity of Integrated Management System	TunTrust Board of Directors
Date :	04/10/2018	19/10/2018	19/10/2018

Table of Contents

1   INTRODUCTION

1.1   OVERVIEW

The Tunisian national agency for digital certification ("TunTrust ") was founded in accordance with Law no. 2000-83 of 9 August 2000 governing electronic exchanges and commerce. TunTrust is a government-owned Certificate Authority (CA) operated in compliance with the international standards.

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

This CP/CPS describes the practices used to comply with the current versions of the following policies, guidelines, and requirements:

− Trust Service Principles and Criteria for Certification Authorities (WebTrust CA), issued by AICPA/CICA in May 2011 (CICA now being CPA Canada since 2012) : http://www.webtrust.org/
− ETSI EN 319 411-1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements : https://www.etsi.org/
− ETSI EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates ; Part 2: Requirements for trust service providers issuing EU qualified certificates : https://www.etsi.org/
− ETSI EN 319 401:Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers https://www.etsi.org/
− Adobe Systems Inc. ("Adobe") AATL Certificate Policy : https://adgrafics.net/,
− The Certification Authority/Browser Forum ("CAB Forum") Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements"): https://cabforum.org/,
− The CAB Forum Network and Certificate System Security Requirements: https://cabforum.org/.

In the event of any inconsistency between the CP/CPS document and these documents, the requirements set out in respective documents take precedence over this document. This CP/CPS document describes execution of the services in regard to accepting certificate applications, certificate issuance and management, certificate revocation procedures, time stamping in compliance with administrative, technical and legal requirements.

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

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

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."

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 http://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

1.3 PKI PARTICIPANTS

TunTrust is a certification authority (CA) that issues digital certificates in accordance with this CP/CPS. As a CA, TunTrust performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses.

TunTrust is also a time stamping authority (TSA) and provides proof-of-existence for data at an instant in time as described in the TP/TPS published in the website http://www.tuntrust.tn/repository. TunTrust CA and TSA operations are managed by the TunTrust Board of Directors. The Board of Directors is responsible for the approval of this CP/CPS and overseeing the conformance of CA and TSA practices with applicable requirements.

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 :
  - o **TnTrust GOV CA** issued by **Tunisia GOV CA** and operates online to issue certificates.
  - o **TnTrust Qualified GOV** issued by **Tunisia GOV CA** and operates online to issue certificates.
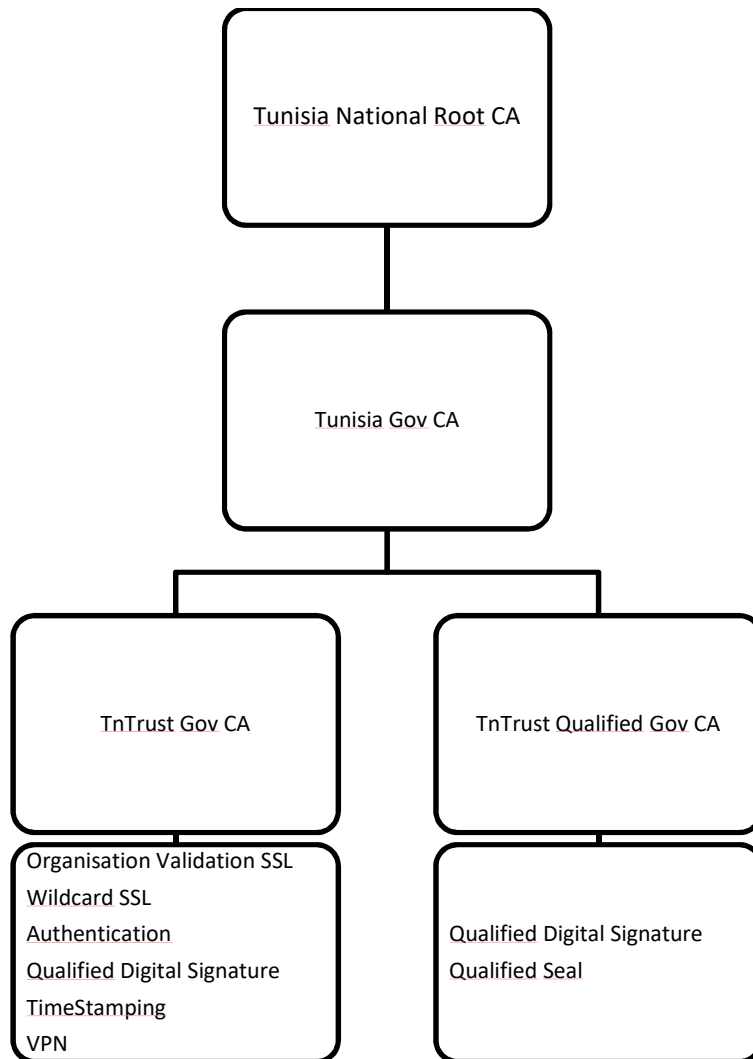
Fig-1: TunTrust CAs Hierarchy

- 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
Organisation Validation SSL	A Certificate to authenticate servers	OVCP OID: 0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.1.1
Wildcard SSL	A Certificate to authenticate servers. Secure SSL certificates that secure multiple hosts on a single domain on the same server.	OVCP OID: 0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.1.1
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	A Certificate to issue an electronic signature that is compliant to EU Regulation No 910/2014 (e-IDAS Regulation) for electronic transactions within the internal European market.	QCP-n-QSCD OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.1
Enterprise-ID	Qualified certificates for electronic seal (eSeal) are intended for the creation of qualified electronic seals in accordance with law no. 272/2016 Coll and EU Regulation no. 910/2014 eIDAS. Qualified certificates for eSeal are issued to legal persons or public authorities, always	QCP-l-QSCD OID: 0.4.0.2042.1.2 OID: 2.16.788.1.2.6.1.10.1.2

	on the hardware device.	

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, a set of Delegated Registration Authorities (DRAs) composed of one or several Physical Verification Point (PVP) and a set of Enterprise Registration Authorities (ERAs).

TunTrust does not enter into agreements with a third party to act as a Registration Authority with SSL certificates issuance or to perform Domain Validation functions as described in sections 3.2.2.4 and 3.2.2.5.

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

Except for SSL certificate performed solely by the CRA, in accordance with Section 3.2.2, TunTrust delegates the performance of certain functions to Delegated Registration Authorities (DRAs) and physical verification point (PVPs).

DRAs and PVPs act under the supervision and control of the CRA.

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,
- Using officially notarized or otherwise authorized documents or sources of information to evaluate and authenticate an Applicant's application,
- 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 is the entity that has final authority and decision upon the issuance and revocation of a Certificate under this CP/CPS. 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)

Delegated RAs have to abide by all the requirements of this CP/CPS. DRAs may, however implement more restrictive practices based on their internal requirements. The DRAs are responsible for the collection of certificate requests and their secure transmission to the CRA.

The Delegated Registration Authorities (DRAs) aim to operate one or several PVPs and proceed, under strictly determined and controlled conditions, to the validation of TunTrust specific face-to-face identification.

Any DRA operating under this CP/CPS must have a contractual agreement with TunTrust which indicates the authorization for their role as DRA and clearly details the minimum requirements, processes and liabilities according to this CP/CPS.

1.3.2.3 PHYSICAL VERIFICATION POINT (PVP)

A Point of Physical Verification always depends on a DRA. The main mission of Physical Verification Points (PVP) is to 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.

Sometimes, the PVPs' functions may be extended to 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: http://www.tuntrust.tn/fr/content/ou-obtenir-mon-certificat

1.3.2.4 Enterprise Registration Authority (ERA)

TunTrust may designate an Enterprise RA to proceed to the registration of the TunTrust new end-entity users (Subscribers) from the Enterprise RA. The ERA's own organization or its subsidiaries. Suitably authenticated account administrators of ERAs must authenticate individuals affiliated with the organization and/or any sub-domains owned or controlled by the organization.

Certificate requests issued by an Enterprise RA must meet the following requirements:

- The requested Fully-Qualified Domain Name(s) are within the Enterprise RA's verified Domain Namespace with confirmation of the CRA.
- If the certificate request includes a Subject name of a type other than a Fully-Qualified Domain Name, the name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject with confirmation of the CRA.

Any ERA operating under this CP/CPS must have a contractual Enterprise agreement with TunTrust which indicates the authorization for their role as ERA and clearly details the minimum requirements, processes and liabilities according to this CP/CPS.

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 verification of identity and issuance of a Certificate, a Subscriber is an Applicant.

Legal Entities are identified on the basis of review of the entity's published by-laws and appointment of director(s) as well as the subsequent government gazette or similar official government publication or other Qualified Independent Information Source (QIIS) or Qualified Government Information Source (QGIS) third party databases. Self-employed Subjects are identified on the basis of proof of professional registration supplied by the competent authority in the Country in which they reside.

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

Relying parties are individuals or organizations that use certificates of any TunTrust CA to validate the signatures and verify the identity of subscribers and/or to secure communication with these subscribers. Relying parties are allowed to use such certificates only in accordance with the terms and conditions set forth in this CP/CPS. It is in their sole responsibility to verify legal validity and applicable policies.

To verify the validity of a digital certificate they received, relying parties must refer to the CRL or OCSP response prior to relying on information featured in a certificate to ensure that the issuing CA under the **Tunisian National Root CA** has not revoked the certificate. The locations of the CRL distribution point and OCSP responder are detailed within the certificate.

Adobe offers the AATL platform from Acrobat® 9.12 and above in order to provide document recipients with improved assurances that certified PDF documents are authentic. Document recipients are Relying Parties who use Adobe products on supported platforms to verify the Subscriber's signature on a certified PDF document. Such detail may be inspected by Relying Parties by using a suitable version of the Adobe PDF reader.

1.3.5 OTHER PARTICIPANTS

No Stipulation.

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.

The applications for which the certificate is deemed to be trustworthy must be decided by the Relying Parties themselves on the basis of the nature and purpose (incl. key usage) of the Certificate, including any applicable limitation as written in the certificate. Complementarily, the relying party must also consider the level of security of the procedures followed for issuance of the Certificate as described in the applicable CP/CPS.

Key usage and the applicability of the certificates are certified (see the description of the Certificate profiles in Section 7).

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 the Tunisian National Agency for Digital Certification via its Board of Directors, acting as Policy Approval Authority. The Board of Directors is composed of the senior management of the Tunisian National Agency for Digital Certification. The procedure used to add or remove members of the Board of Directors is determined and ruled by internal documents.

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 Certification Practice Statement(s), TunTrust Certificate Policies and TunTrust Time Stamping Policies.
- Defining the review process for practices and policies including responsibilities for maintaining the Certification Practice Statements and Certificate.
- Defining the review process that ensures that the TunTrust CAs properly implements the above practices.
- Defining the review process that ensures that the Certificate Policies are supported by the TunTrust Practice Statement(s).
- Publication to the Subscribers and Relying Parties of the Certificates Policies and Certification Practice Statements and their revisions.

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

> TUNTRUST - National Agency for Digital Certification
> Technopark El Ghazala,
> Road of Raoued,
> Ariana, 2083
> Tunisia.
>
> Tel.: +216 70 834 600
> Mail: ndca.pki@tuntrust.tn
> Web: http://www.tuntrust.tn

1.5.2 CONTACT PERSON

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

> PKI Policy Manager,
>
> ndca.pki@tuntrust.tn

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

1.5.3 PERSON DETERMINING CP/CPS SUITABILITY FOR THE POLICY

The Entity determining CP/CPS suitability is TunTrust, via its TunTrust Board of Directors acting as Policy Approval Authority based on the results and recommendations received from an independent auditor (see Section 8).

1.5.4 CP/CPS APPROVAL PROCEDURE

The Entity approving the CP/CPS is TunTrust, via its TunTrust Board of Directors acting as Policy Approval Authority. See section 1.5.1 for contact details. The procedure used to approve documents is determined and ruled by internal documents.

TunTrust Board of Directors determines whether an amendment to this CP/CPS requires notice or an OID change. See also Section 9.12 below.

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

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.

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 may log SSL Certificates with a public certificate transparency database. 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.

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.

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, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or if there is clear evidence that the specific method used to generate the Private Key was flawed.

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.

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 8.3.

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 http://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

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.

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 these 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

2   PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1   REPOSITORIES

TunTrust is the ultimate entity responsible for the operation of online and publicly available repository (ies). TunTrust is also responsible for the publication of the following documents and information:

- − The CP/CPS (Certificate Policies and Certification Practice Statement);
- − The related subscriber contractual agreements (e.g: Subscriber Agreement, etc.);
- − The Certification Authority Certificates, Certification Paths and related ARLs;
- − The Certificates Public Registry;
- − The Certificate Revocation Lists (CRLs);

The aforementioned documents as well as complementary information are available from online publicly accessible website on http://www.tuntrust.tn/repository as described in section 2.2.

TunTrust makes best endeavors to ensure that the uptime of the repository exceeds 99,0%.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

TunTrust publishes information related to certificates issued by TunTrust CAs on its publicly accessible website http://www.tuntrust.tn/. The TunTrust web site and the LDAP directory ldap://ldap.tuntrust.tn are the only authoritative sources for:

- All publicly accessible certificates issued by the TunTrust CAs.
- The certificate revocation list (CRL) for the TunTrust CAs. The CRL is downloaded from the http://crl.tuntrust.tn web site. The exact URL is documented in every certificate that is issued by TunTrust CAs in the field: "CRL Distribution Point". Meanwhile, subscriber or relying party can get the current state of certificate instantly via OCSP service (va.tuntrust.tn) provided by TunTrust CA.

The data formats used for certificates issued by TunTrust CAs and for certificate revocation lists in the TunTrust web site are in accordance with the associated schema definitions as defined in the X.500 series of recommendations.

In addition, TunTrust publishes test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. These test Web pages are accessible at the following URLs:

TunTrust Gov CA:

> for valid Certificate https://valid-gov-ov.tuntrust.tn/

> for revoked Certificate https://revoked-gov-ov.tuntrust.tn/

> for expired Certificate https://expired-gov-ov.tuntrust.tn/

2.3 TIME OR FREQUENCY OF PUBLICATION

TunTrust develops, implements, enforces, and annually updates the CP/CPS to meet the latest version of the requirements.

Internal and external audit activities are achieved every year, that conduct to a regular review of the CP/CPS.

2.4 ACCESS CONTROLS ON REPOSITORIES

TunTrust makes its Repository publicly available in a read-only manner.

Logical and physical security measures are implemented to prevent unauthorized persons from adding, deleting, or modifying repository entries. TunTrust is the only entity that has write access to Repositories.

3 IDENTIFICATION AND AUTHENTICATION

TunTrust implements rigorous authentication requirements to ensure that the identity of the Applicants is proven. This may include face-to-face identity verification at the beginning of the Certificate request procedure or at some point prior to Certificate issuance. The registration procedure will depend on the type of Certificate that is being applied for.

3.1 NAMING

3.1.1 TYPES OF NAMES

All certificates contain a differentiated X.501 name in the Subject field, including a Common Name component (CN=) relating to the identity of the subscriber and identified in the certificate, as well as additional pieces of identity information in the SubjectAlternativeName field.

The DN contained in the certificates is those listed below:

3.1.1.1 ID-TRUST CERTIFICATE

Field	M/O[1]	Value
serialNumber	M	Serial Number as constructed by TunTrust
commonName	M	Concatenation of given name and surname as in ID card separated by a "space" character.
givenName	O	Given Name as on ID card
Surname	O	Surname as on ID card
countryName	M	Nationality of holder (ISO3166)
emailAddress	M	Subject's email address
OrganizationName	O	**For Professional certificates :** Name of company/institution.
OrganizationalUnitName	O	**For Professional certificates :** Company department or other information item

3.1.1.2 ENTERPRISE-ID CERTIFICATE

Field	M/O	Value
serialNumber	M	Serial Number as constructed by TunTrust CRAO
commonName	M	Contains the full registred name of the subject (legal person)
countryName	M	Nationality of holder (ISO3166)
OrganisationIdentifier (2.5.4.97)	M	Contains information using the following structure in the presented order: - 3 character legal person identity type reference; VAT - 2 character ISO 3166 country code; - hyphen-minus "-" and - Tax Identification number
OrganizationName	M	Contains the full registred name of the subject (legal person).

---

[1] M : Manadatory / O: Optional

OrganizationalUnitName	O	Company department or other information item

3.1.1.3 TUNTRUST OV SSL/TLS CERTIFICATE

Field	M/O	Value
serialNumber	M	Serial Number as constructed by CRAO
commonName	O	FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or unique name of server.
countryName	M	Nationality of holder (ISO3166)
localityName	M	Location in which the company's registered office is established.
OrganizationName	M	Contains the full registered name of the
OrganizationalUnitName	O	Company department or other information item
E-mail	O	E-mail address Server Administrator

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

TunTrust uses distinguished names 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 the registration authority 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. The Issuing CA may, if necessary, insert additional numbers or letters to the Subscriber's Subject Common Name, or other attribute, in order to distinguish between two Certificates that would otherwise have the same Subject Name.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

TunTrust issuing CAs are not obligated to seek evidence of trademark usage by any Organization.

3.2 INITIAL IDENTITY VALIDATION

Initial Identity validation is part of the certificate application process described in chapter 4.1. Initial identity validation procedures for PKI Participants or organization of PKI Participants other than subscribers, comply with provisions of the CP/CPS (and in particular with section 5.2.1).

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

3.2.1.1 CERTIFICATES FOR DEVICES

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

3.2.1.2 CERTIFICATES FOR PERSONS

Certificates for persons are issued under the CRA's direct control on behalf of the Subscriber. The key generation is performed on a compliant QSCD container such as PKI smartcard or crypto token. In this case, 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.

For all certificate enrollment requests, TunTrust issuing CAs performs the digital signature validation checks to ensure it is a properly formed message and that its integrity has not been altered.

In cases where key generation is performed under the CRA's direct control proof of private key possession is not required.

3.2.2 AUTHENTICATION OF ORGANIZATION AND DOMAIN IDENTITY

TunTrust verifies organization identity and address using documentation or through communication with at least one of the following : (i) A government agency (QGIS) in the jurisdiction of the Applicant, or a superior governing governmental agency if the Applicant claims they are a government agency themselves, (ii) A third party database that is periodically updated and has been evaluated by TunTrust to determine that it is reasonably accurate and reliable; or (iii) A Qualified Governmental Tax Information Source.

In case of foreign law companies, an additional banking reference can be required and TunTrust reserves right to reject the application of such companies.

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 commercial register not older than 3 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) A copy of the identity evidence (identity card, passport or Tunisia residency card) of the Server Administrator.

d) 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.

e) 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. Constitutive act, or recent extract from the commercial register 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. An Attestation Letter accompanied by documentary support.

3.2.2.3 VERIFICATION OF COUNTRY

TunTrust verifies the country associated with the Subject using one of the following: (a) the ccTLD of the requested Domain Name; (b) information provided by the Domain Name Registrar; or (c) a method identified in Section 3.2.2.1.

3.2.2.4 VALIDATION OF DOMAIN AUTHORIZATION OR CONTROL

TunTrust validates the Applicant's right to use the domain name using at least one of these methods compliant with BR.: (i) Email or SMS to Domain Contact, (ii) Phone Contact With Domain Contact, (iii) Constructed Email To Domain Contact.

TunTrust does not support .onion domains at this time.

3.2.2.4.1 EMAIL TO DOMAIN CONTACT

TunTrust confirms the Applicant's control over the FQDN or Wildcard Domain Names by sending a Random Value via email to one recipient or more identified as a Domain Contact, and then receiving a confirming response utilizing the Random Value. Each email may confirm control of multiple Authorization Domain Names.

The RANDOM VALUE is unique in each email. TunTrust may resend the email in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged. The Random Value remains valid for use in a confirming response for no more than 30 days from its creation.

If the FQDN has been validated using this method, TunTrust may also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.2.4.2 PHONE CONTACT WITH DOMAIN CONTACT

TunTrust confirms the Applicant's control over the FQDN or Wildcard Domain names by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN.

TunTrust places the call to a phone number identified by the Domain Name Registrar as the Domain Contact. Each phone call is made to a single number and may confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

Once the FQDN has been validated using this method, TunTrust may also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.2.4.3 CONSTRUCTED EMAIL TO DOMAIN CONTACT

TunTrust confirms the Applicant's control over the FQDN or Wildcard Domain names by sending an email including a unique Random Value to Domain Contact created by using 'admin'|'administrator'|'webmaster'|'hostmaster'|'postmaster'@'Authorization Domain name', and receiving a response using the Random Value.

Each email may confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The email with no content and no recipient modification may be re-sent in its entirety, including the re-use of the Random Value.

The Random Value remains valid for use in a confirming response for no more than 30 days from its creation.

Once the FQDN has been validated using this method, TunTrust may also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.2.5 AUTHENTICATION FOR AN IP ADDRESS

Not Applicable.

3.2.2.6 WILDCARD DOMAIN VALIDATION

If the FQDN contains a wildcard character, then TunTrust issuing CAs remove all wildcard labels from the left most portion of requested FQDN. TunTrust issuing CAs 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.

Before issuing a certificate with a wildcard character in a CN or subjectAltName of a type DNS-ID, TunTrust issuing CAs follow an internal documented procedure that determines if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation).

If a wildcard would fall within the label immediately to the left of a registry-controlled or public suffix, the TunTrust issuing CAs refuses issuance unless the applicant proves its rightful control of the entire Domain Namespace.

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 automaticaly through administrative authorities services to ensure the accuracy of information.

3.2.2.8 CAA RECORDS

Prior to issuing SSL Digital Certificates, TunTrust checks for CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued.

TunTrust may not check CAA records for the following exceptions:

− For Certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked.
− For Certificates issued by a Technically Constrained Issuing CA Certificate, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.
− If the CA or an Affiliate of the CA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

TunTrust treats a record lookup failure as permission to issue if:
− the failure is outside the TunTrust 's infrastructure;
− the lookup has been retried at least once; and
− the domain's zone does not have a DNSSEC validation chain to the ICANN root

TunTrust documents potential issuances that were prevented by a CAA record, and will dispatch reports of such issuance requests to the contact stipulated in the CAA iodef record(s), if present. TunTrust supports mailto: and https: URL schemes in the iodef record.

The identifying CAA domain for TunTrust is 'tuntrust.tn'.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

TunTrust implements rigorous authentication requirements to ensure that the identity of the Applicant is proven. This includes face-to-face identity verification at the beginning of the Certificate request procedure or at some point prior to Certificate issuance to the Subscriber.

A face-to-face identification 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.

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

− The CRAO/PVPO must verify the authenticity and validity of the provided identity proof according to procedures provided by TunTrust.

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.

When phone number and email address are to be listed in the Applicant Certificate, TunTrust performs the following verification:

- Applicant's ability to place and receive calls from the provided phone number;
- Applicant's control of the email address listed in the certificate by sending a random Value via email and then receiving a confirming response utilizing the Random Value. TunTrust may resend the email in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged. The Random Value remains valid for use in a confirming response for no more than 30 days from its creation. For corporate email certificates, TunTrust verifies the organization and domain name listed in the certificate similar to an SSL Server Certificate. The organization is required to request revocation of the Certificate when that affiliation ends.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

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

3.2.5 VALIDATION OF AUTHORITY

Where an Applicant's Name is to be associated with an Organizational Name to indicate his or her status as a Counterparty, Employee or specifies an Authorization level to act on behalf of an Organization, the Registration Authority will validate the Applicant's Authority by reference to business records maintained by the Registration Authority, its Subsidiaries, Holding Companies or Affiliates. Validation of authority is conducted in compliance with this CP/CPS. Validity of authority of Applicant Representatives and Agents is verified against contractual documentation and Reliable Data Sources.

3.2.6 CRITERIA FOR INTEROPERATION

No Stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

Subscribers may request re-key of a Certificate prior to a Certificate's expiration. The subscriber identifies and authenticated himself for routine re-keying with the valid certificate and the possession of the corresponding private key. After receiving a request for re-key, TunTrust creates a new Certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the Certificate has an extended validity period, TunTrust may perform some revalidation of the Applicant but may also rely on information previously provided or obtained. Identification and authentication for re-key after revocation

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

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The Subscriber, and if applicable the legal representative (or his duly appointed delegate) of the company / organization from which the Subscriber is a member off the CRA or TunTrust CA may apply for revocation of the Certificate. The Subscriber (or the Subject, when different) is notified by email upon certificate status change.

Revocation requests from Subscriber may be granted if the Subscriber is authenticated according to one of the following methods:

- Providing a challenge value associated with certificate
- Personal appearance at the CRA or PVP.

The process how the revocation request can be submitted is described in section 4.9.3.

Issuing CAs 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 or non- payment of applicable fees.

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

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

Within the context of new Applicant registration, the CRA responsibility is to verify that the Applicant is indeed the person (s) he claims to be and to validate the information that is requested to be certified by issuing CAs as well as the information supporting this certification. This shall be done in compliance with the rules and practices as stated by this CP/CPS and by strictly following the TunTrust registration procedures or the applicable national law.

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.

Upon successful face-to-face identification of the Applicant, the PVP officer combines and securely transmits the submitted documents to the corresponding DRA. The DRA then performs an additional check of the submitted documents prior to transmission to the CRA. The CRA proceeds to the verification and validation of all documents submitted by the Applicant. In case the professional quality has to be certified, the CRA will verify and validates Applicant's professional quality as described in section 3.2.

The CRA guarantees the accuracy of all information contained in the certificate request sent to TunTrust issuing CAs. It also guarantees that the certificates Subscriber as well as the certificate Subject (in case the Subject and the Subscriber of the certificate are different entities) have been duly registered and that all required verifications have been performed prior to successful registration leading to Certificate issuance.

4.1.2.1 SUBSCRIBER ENROLLMENT PROCESS

4.1.2.1.1 REGISTRATION PREPARATION

As a general provision, the Subscriber must obtain the Order Form and the Subscriber Agreement for the Certificate (hereafter referred to as "the Order Form" and "the Subscriber Agreement") from TunTrust.

These, together with the present CP/CPS, form the Subscriber Agreement between the Subscriber and TunTrust. The present CP/CPS, Order Forms and Subscriber Agreement for Certificates issued by TunTrust are available for download at https://www.tuntrust.tn/repository. The Subscriber must duly complete and sign the Order Form and the Subscriber Agreement.

The Order Form may fall into two parts:

− The "Subscriber Part" must be duly completed and signed by the Subscriber.
− If applicable (optional): The "Subscriber Organization Part" must be duly filled in and signed by a legal representative (or his/her duly appointed proxy) of the organization to which the Subscriber belongs.

By signing the Order Form and the Subscriber Agreement, the Subscriber and, if applicable, the Subscriber's organization accept the present CP/CPS.

4.1.2.1.2 ONLINE REGISTRATION PREPARATION

In order to ease Subscriber registration preparation and to reduce the amount of errors, an end-user web-based registration preparation interface is provided to the Subscriber at https://mpki.tuntrust.tn. It requires users to maintain an account with a suitably strong username and password for ongoing maintenance of the lifecycle of the Certificate. The account may be classified as Individual, EPKI or Reseller. An Applicant must submit an application via a secure ordering process according to a procedure maintained by TunTrust.

The MPKI interface presents the Subscriber with a convenient & intelligent electronic form to collect information needed for registration. This form will dynamically present appropriate fields in function of the choices of the Subscriber: type of requested certificate, type of identity (e.g., physical private person or physical person with professional attributes), type of requested Signature Creation Device (e.g., HSM, or crypto token), etc.

4.1.2.2 RESPONSIBILITIES RELATED TO ENROLLMENT PROCESS

4.1.2.2.1 SUBSCRIBERS' RESPONSIBILITIES

By signing the Subscriber Agreement the Subscriber agrees with and accepts the associated Subscriber Agreement and the applicable CP/CPS. Specifically, the Subscriber hereby gives his/her acceptance to the following responsibilities related to the enrolment process:

− Having a basic understanding of the proper use of public key cryptography and certificates;
− Providing only correct information without errors, omissions or misrepresentations;
− Substantiating information by providing a properly completed and personally signed order form;
− Supplementing such information with a proof of identity and the provision of the information as specified in section 3;
− Verifying the content of a newly issued certificate before its first use and to refrain from using it, if it contains misleading or inaccurate information.
− Reading and agreeing to all terms and conditions of this CP/CPS and other relevant regulations and agreements;
− Ensuring complete control over the private key by not sharing private keys and passwords;
− Notifying TunTrust of any change to any of the information included in the certificate or any change of circumstances that would make the information in the certificate misleading or inaccurate;

− Invalidating the certificate immediately if any information included in the certificate is misleading or inaccurate, or if any change of circumstances, makes the information in the certificate misleading or inaccurate;

− Notifying TunTrust immediately of any suspected or actual compromise of the private key and requesting that the certificate be revoked;

− Immediately ceasing to use the certificate upon (a) expiration or revocation of such a certificate, or (b) any suspected or actual damage/corruption of the private key corresponding to the public key in such a certificate, and immediately removing such a certificate from the devices and/or software onto which it has been installed;

− Refraining to use the subscriber's private key that corresponds to the public key certificate to sign other certificates;

− Protecting the private key from unauthorized access;

− If the Certificate requires the use of a Qualified Electronic Signature Creation Device (QSCD) or Cryptographic Module, for example for the creation of digital signatures, the Subscriber must use the Certificate with such a device that either been supplied by or approved by TunTrust;

− If the Subscriber generates their keys, then they will generate them in a secure manner in accordance with industry leading practices.

4.1.2.2.2 CRA RESPONSIBILITIES

When face-to-face registration is required, the CRA, DRA, ERA and PVP (hereafter referred to as TunTrust RAs) are either under a contractual obligation or regulated by the national law to comply scrupulously with the registration procedures described in related TunTrust internal PVP procedures and the TunTrust internal CRA procedures.

The CRA guarantees that:

− Subscribers are properly identified and authenticated both with regard to the personal identity of the Subscriber as a natural private person and with regards to any optional information about optional professional status.

− Any application for Certificates submitted to the CA is complete, accurate, valid and duly authorized, in particular for Certificate Subject related information when the Subject and the Subscriber of the requested Certificate are different entities.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

Certificate type	Enrollment process
ID-Trust for private person with no professional attributes	• Applicant must physically present himself to CRA/PVP officer in order to carry out face-to-face identification and must bring with him/her : a) Order Form and Subscriber Agreement signed by Applicant; b) Copy of national ID photo (identity card, passport or Tunisia residency card)

Certificate type	Enrollment process

	• CRA/PVP officer inspects the national ID photo provided by Applicant, and verifies that the Order Form is duly filled in and signed.
	
	• Upon successful face-to-face identification of Applicant, PVP officer combines and securely transmits the submitted documents to the corresponding DRA for final secure transmission to the CRA.
	
	• The CRA proceeds to the verification and validation of all documents submitted by the Applicant. In particular, The CRA verifies that the Applicant has control over the email address to be listed within the Certificate through a challenge response mechanism.
	
	• Upon successful validation of the Applicant identity, the CRA initiates the certificate request to the Issuing CA following these steps:
	
	   a. The CRAO performs the personalization of the TunTrust QSCD with on-board key-pair generation, in the presence of the Subscriber or his duly mandated representative. The key-pair generation may also be done by CRAO on behalf of the Applicant.
	
	   b. The CRAO initiates the certificate request to the *TnTrust Qualified GOV CA* via the Token Management System.
	
	   c. The CRAO installs the issued certificate in the TunTrust QSCD via the Token Management System.
	
	   d. The CRAO delivers the TunTrust QSCD to Applicant himself or to a duly mandated representative of the Applicant or QSCD is securely transmitted to the PVP where Applicant submitted his certificate request.
	
	Upon termination of the certificate request process, CRA combines and securely stores Applicant submitted data

ID-Trust for physical person with professional attributes	• Applicant must physically present himself to CRA/PVP/ERA officer in order to carry out face-to-face identification and must bring with him/her :
	
	   a. 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.
	
	   b. Constitutive act, or recent extract of the commercial register not older than 3 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.
	
	   c. Subscriber Agreement signed by Applicant;
	
	   d. Copy of national ID photo of Applicant (identity card, passport or

Certificate type	Enrollment process
	Tunisia residency card)
	• CRA/PVP/ERA officer inspects the national ID photo provided by Applicant, and verifies that the Order Form is duly filled in and signed.
	• Upon successful face-to-face identification of Applicant, PVP officer combines and securely transmits the submitted documents to the corresponding DRA for final secure transmission to the CRA. Upon successful face-to-face identification of Applicant, ERA officer combines and securely transmits the submitted documents to the CRA.

	• The CRA proceeds to the verification and validation of all documents submitted by the Applicant. In particular, The CRA verifies the following :
	
	  a. The Applicant is affiliated with the organization and that the Applicant has the authority to possess a certificate indicating the affiliation as described in section 3.2.2.
	
	  b. The Applicant has control over the email address to be listed within the Certificate through a challenge response mechanism.

	• Upon successful validation of the Applicant identity, the CRA initiates the certificate request to the Issuing CA following these steps:
	
	  a. The CRAO performs the personalization of the TunTrust QSCD with on-board key-pair generation, in the presence of the Subscriber or his duly mandated representative. The key-pair generation may also be done by CRAO on behalf of the Applicant.
	
	  b. The CRAO initiates the certificate request to the **TnTrust Qualified GOV CA** via the Token Management System.
	
	  c. The CRAO installs the issued certificate in the TunTrust QSCD via the Token Management System.
	
	  d. The CRAO delivers the TunTrust QSCD to Applicant himself or to a duly mandated representative of the Applicant or QSCD is securely transmitted to the PVP where Applicant submitted his certificate request.
	
	  e. Upon termination of the certificate request process, CRA combines and securely stores Applicant submitted data.

Enterprise-ID	• Applicant must physically present himself to CRA/PVP/ERA officer in order to carry out face-to-face identification and must bring with him/her : a. 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.

Certificate type	Enrollment process

	b. Constitutive act, or recent extract of the commercial register not older than 3 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.
	
	c. Subscriber Agreement signed by Applicant;
	
	d. Copy of national ID photo of Applicant (identity card, passport or Tunisia residency card).
	
	• CRA/PVP/ERA officer inspects the national ID photo provided by Applicant, and verifies that the Order Form is duly filled in and signed.
	
	• Upon successful face-to-face identification of Applicant, PVP officer combines and securely transmits the submitted documents to the corresponding DRA for final secure transmission to the CRA. Upon successful face-to-face identification of Applicant, ERA officer combines and securely transmits the submitted documents to the CRA.
	
	• The CRA proceeds to the verification and validation of all documents submitted by the Applicant. In particular, The CRA verifies that the Applicant is affiliated with the organization and that the Applicant has the authority to possess a certificate indicating the affiliation as described in section 3.2.2.
	
	• Upon successful validation of the Applicant identity, the CRA initiates the certificate request to the Issuing CA following these steps:
	
	    a. The CRAO performs the personalization of the TunTrust QSCD with on-board key-pair generation, in the presence of the Subscriber or his duly mandated representative. The key-pair generation may also be done by CRAO on behalf of the Applicant.
	
	    b. The CRAO initiates the certificate request to the *TnTrust Qualified GOV CA* via the Token Management System.
	
	    c. The CRAO installs the issued certificate in the TunTrust QSCD via the Token Management System.
	
	    d. The CRAO delivers the TunTrust QSCD to Applicant himself or to a duly mandated representative of the Applicant or QSCD is securely transmitted to the PVP where Applicant submitted his certificate request.
	
	Upon termination of the certificate request process, CRA combines and securely stores Applicant submitted data.

TunTrust OV SSL	• Applications for OV SSL Certificates shall be submitted by either 1) the administrative, registrant, or technical contact associated with the WHOIS

Certificate type	Enrollment process

	record for the domain.
	To obtain a TunTrust SSL Certificate, an Applicant must:
	    (i) generate a secure and cryptographically Key Pair,
	    (ii) complete and submit a TunTrust SSL Certificate Application (i.e. an "Order Form"), providing all information requested by a TunTrust CRA without any errors, misrepresentation, or omissions ; and
	    (iii) agree with the Subscriber terms and conditions (which is made of the relevant Order Form, the Subscriber Agreement and the applicable CP/CPS).
	
	• OV SSL certificate applications includes the following:
	
	  a. Order Form duly completed and signed by Applicant legal representative
	
	  b. Constitutive act, or recent extract of the commercial register not older than 3 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.
	
	  c. Subscriber Agreement signed by Applicant;
	
	  d. Copy of national ID photo of Applicant (identity card, passport or Tunisia residency card)
	
	  e. The Certificate Signed Request (CSR)
	
	• The CRAO proceeds to the verification and validation of all documents submitted by the Applicant as specified in section 3.2.
	
	• The CRAO initiates the certificate request to the **TnTrust GOV CA**.
	
	• The CRAO delivers the TunTrust SSL certificate to the Applicant himself or to a duly mandated representative of the Applicant.
	
	Upon termination of the certificate request process, CRA combines and securely stores Applicant submitted data

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

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

From time to time, TunTrust may modify the requirements related to application information requested, based on TunTrust requirements, business context of the usage of Certificates, or as may be required by law, or changes to the Baseline Requirements.

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 CAs will verify:

- The integrity of the request;
- The authenticity and authority of the CRA operator; TunTrust CAs only accept requests sent by TunTrust CRA officers with trusted roles capable of causing Certificate issuance using multi-factor authentication.
- The contents of the certificate requests for compliance with the technical specification as outlined in section 7.1.2.

TunTrust logs SSL Certificates intended to be trusted in Chrome in two or more Certificate Transparency databases.

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

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

The Applicant will be notified that the Certificate is issued via email which 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.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

Certificate acceptance is governed by and should comply with the practices described in, and any requirements imposed by this CP/CPS.

Until a Certificate is accepted, it is not published in any Repository or otherwise made publicly available. By using a Certificate, the Subscriber thereof certifies and agrees to the statements contained in the notice of acceptance. This CP/CPS sets out what constitutes acceptance of a Certificate. An Applicant that accepts a Certificate warrants to the relevant Issuing CA, and all Authorized Relying Parties who reasonably rely, 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 TunTrust 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.

4.4.2 NOTICE OF ACCEPTANCE

By accepting a certificate, the certificate holder acknowledges that he or she agrees to the terms and conditions contained in this certificate policy & certification practice statement and the applicable user agreement. Also by accepting a certificate, the subscriber assumes a duty to retain control of the private key corresponding to the public key contained in the certificate, to use a trustworthy system and to take reasonable precautions to prevent the private key's loss, exclusion, modification, or unauthorized use.

4.4.3 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

The subscriber is responsible for installing the issued certificate on the subscriber's computer or security module according to the subscriber's system specifications. A subscriber is deemed to have accepted a certificate when: The subscriber uses the certificate; or 30 days pass since issuance of the certificate.

4.4.4 PUBLICATION OF THE CERTIFICATE BY THE CA

As specified in Section 2 (Publication and Repository Responsibilities) of this CP/CPS, all Certificates issued by TunTrust are made available in public repositories.

4.4.5 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

No Stipulation.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

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

Subscribers use private keys in accordance with the key usage field extension. End-user subscriber is bound to use the certificate for its lawful and intended purposes only.

Where it is possible to make a backup of a Private Key, Subscribers must use the same level of care and protection attributed to the live Private Key. At the end of the useful life of a Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Within this CP/CPS, 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 an Authorized 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.

4.6.2 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

Not Applicable.

4.6.3 WHO MAY REQUEST RENEWAL

Not Applicable.

4.6.4 PROCESSING CERTIFICATE RENEWAL REQUESTS

Not Applicable.

4.6.5 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable.

4.6.6 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

Not Applicable.

4.6.7 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

Not Applicable.

4.6.8 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable.

4.7 CERTIFICATE RE-KEY

Certificate re-keying is a process where a Subscriber automatically obtains a new certificate if proof of key possession of the old certificate can be provided. The resulting certificate contains new validity information, a new key pair but retains the same subject.

If the legal and regulatory requirements governing the certificate to be issued and the stipulations in this CP/CPS are met, TunTrust supports re-key and re-issue of certificate.

TunTrust may choose to allow changes to the information contained in the subject, if all changes are validated and authorized.

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

4.7.1.1 RE-KEY OF DEVICE CERTIFICATES

No Stipulation.

4.7.1.2 RE-KEY OF END-USER CERTIFICATE

No Stipulation.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

No Stipulation.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUEST

No Stipulation.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

No Stipulation.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

No Stipulation.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

No Stipulation.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

No Stipulation.

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.

4.9 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 by posting the serial number of the Certificate to a Certificate Revocation List.

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;
d) TunTrust obtains evidence that the Certificate was misused;
e) TunTrust is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;

f) TunTrust is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name 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);

g) TunTrust is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;

h) TunTrust is made aware of a material change in the information contained in the Certificate;

i) TunTrust is made aware that the Certificate was not issued in accordance with these Requirements CP/CPS;

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

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

l) 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;

m) TunTrust is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;

n) Revocation is required by the TunTrust's CP/CPS; or

o) The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

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; Forum Guideline Baseline Requirements, v. 1.5.7 27

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;

i) Revocation is required by TunTrust CP/CPS; or

j) The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

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 an affiliated organization named in the Certificate. 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. TunTrust may also at its own discretion revoke Certificates.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

TunTrust will revoke a Certificate upon receipt of a valid request. A revocation request should be promptly and directly communicated to TunTrust and the Registration Authority that approved or acted in connection with the issue thereof. The Subscriber may be required to submit the revocation request via the TunTrust Support Line or directly over an Internet connection. The TunTrust website (http://www.tuntrust.tn) provides a mechanism in which to submit revocation requests. The Subscriber, is required to provide a shared secret that will be used to activate the revocation process.

The Subscriber can also personally visit the TunTrust CRA and requests the revocation of a certificate off line. The subscriber presents a valid ID photo for identification purposes. A revocation request may be communicated electronically if it is digitally signed with the Private Key of the Subscriber requesting revocation (or the Organization, where applicable).

TunTrust maintains a continuous 24/7 ability to internally respond to any high priority Certificate Problem Report and will take such action as deemed appropriate based on the nature of such a report. This may include, but not be limited to, the revocation of a Certificate that is the subject of such a complaint.

4.9.4 REVOCATION REQUEST GRACE PERIOD

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

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

For a Certificate Problem Report, TunTrust will begin investigation within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on the following criteria:

a) The nature of the alleged problem;
b) The number of Certificate Problem Reports received on a particular Certificate or Subscriber;
c) The entity making the complaint;
d) Relevant legislation.

4.9.6 REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

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

4.9.7 CRL ISSUANCE FREQUENCY

For the status of TunTrust CAs certificates:

TunTrust updates and reissues CRLs at least (i) once every twelve months and (ii) within upon revoking a Subordinate CA Certificate, and the value of the next Update field MUST NOT be more than twelve months beyond the value of this Update 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 next Update field must not be more than ten days beyond the value of this Update 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 CAs are issued according to section 4.9.7 and published in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

TunTrust supports OCSP responses in addition to CRLs. Response times are generally no longer than 10 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.

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. Outside system maintenance windows, system failure or other factors which are not under the control of TunTrust CA, the TunTrust CA shall make best endeavors to ensure that the uptime of these services exceeds 99,0%.

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

No stipulation.

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

No Stipulation.

5 MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

This section of the CP/CPS outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use by TunTrust to provide trustworthy and reliable CA operations.

TunTrust has implemented a Security Policy, which supports the security requirements of this CP/CPS. Compliance with these policies is included in independent audit requirements described in section 8.

TunTrust carries out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. This risk analysis performed with the full support and collaboration of all component services providers and is regularly reviewed and revised if necessary. This risk analysis is available as an internal document.

TunTrust, acting as TSP including activities, provides direction on information security through its Board of Directors, responsible for defining the information security policy and ensuring publication and communication of the policy to all personnel who are impacted by the policy.

This information security policy is implemented with the full support and collaboration of all component services providers and is regularly reviewed and revised if necessary. Appropriate systems, infrastructures and measures for quality and information security management are implemented and maintained at all times. Any changes that would impact on the level of security provided must be approved by TunTrust through its TunTrust Board of Directors. The TunTrust information security policy as well as documentation on security controls and operating procedures is available as separate and internal documents.

TunTrust ensures implementation and maintains appropriate level of protection to its assets and information systems. For this purpose TunTrust maintains an inventory of all information assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis.

5.1 PHYSICAL CONTROLS

5.1.1 SITE LOCATION AND CONSTRUCTION

TunTrust CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information.

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 a data center that has 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 center is 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, fire, and electromagnetic.

5.1.7   WASTE DISPOSAL

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

5.1.8   OFF-SITE BACKUP

TunTrust performs routine backups of critical system data, and other sensitive information. The backed up data are stored in a physically secured offsite locations.

5.2   PROCEDURAL CONTROLS

5.2.1   TRUSTED ROLES

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

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

- **Registration and Customer Services Responsible (Operator)**

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

- **PKI Administrator**

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

- **System Administrator**

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

- **Physical and Logical Security Officer**

The Physical Security Officer is a trusted role. He 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).

- **Customer Support Personnel (Operator)**

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

- **Auditor**

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

- **Key Manager**

The Key Manager is a trusted role. He is responsible of conducting the key ceremonies.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

Two or more persons are required by TunTrust CAs for the following tasks:

(a) CA key generation = Three (3) persons

(b) CA signing key activation = Two (2) persons

(c) CA private key backup = Three (3) persons

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

Multiparty control for logical access is not achieved using personnel that serve in the Auditor Trusted Role.

HSM Administrators uses HSM Smartcards for authentication. The HSM itself enforces dual control based on the HSM smartcards for the different functions. The number of needed HSM-smartcards (m) of the total number of produced HSM-smartcards (n) will be:

(a) Key generation = 3 of 6

(b) Signing key activation = 2 of 8

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

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

Before appointing a person to a trusted role, TunTrust performs a background check. Each role described above is identified and authenticated in a manner to guarantee that the right person has the right role to support the CA.

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES
Roles requiring a separation of duties include:
1. Those performing authorization functions such as the verification of information in certificate applications and approvals of certificate applications and revocation requests,
2. Those performing physical and logical security functions;
3. Those performing audit ; and
4. Those performing duties related to system administration.

To accomplish this separation of duties, TunTrust specifically designates individuals to the trusted roles defined in Section 5.2.1 above.

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 in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, TunTrust verifies the identity and trustworthiness of such person.

5.3.2 BACKGROUND CHECK PROCEDURES

TunTrust verifies the background of its employees covering the following areas:

(a) Employment

(b) Education and Certification

(c) Place of residence

(d) Law Enforcement

(e) References

TunTrust will not appoint any person who is known to have been convicted of a serious crime or other offense which could affect his suitability for the position. TunTrust will ask any candidate to provide such information and refuse an application if access to such information is denied.

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 CAB 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.

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 (awareness) plan, and the execution of such plan is documented.

TunTrust provides 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

Contractor personnel employed for TunTrust CA operations are subject to the same process, procedures, assessment, security control and training as permanent CA personnel.

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.

Documentation is maintained identifying all personnel who received training and the level of training completed.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 TYPES OF EVENTS RECORDED

TunTrust and each Delegated Third Party records 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 the CAB Forum and the CA's Certification Practice Statement;

    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;

    d. Acceptance and rejection of certificate requests;

    e. Issuance of Certificates; and

    f. Generation of Certificate Revocation Lists and OCSP entries.

3. Security events, including:

    a. Successful and unsuccessful PKI system access attempts;

    b. PKI and security system actions performed;

    c. Security profile changes;

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

    e. Firewall and router activities; and

    f. Entries to and exits from the CA facility.

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

Audit logs are reviewed periodically for any evidence of malicious activity and following each important operation.

Audit logs are archived continuously.

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

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 individuals with authorized trusted 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. Audit log backup is protected to the same degree as originals.

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

No stipulation.

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 also performs regular vulnerability assessment and penetration testing covering all TunTrust assets related to Certificate issuance, products and services. Assessments focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration or destruction of the Certificate issuance process.

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF RECORDS ARCHIVED

The following records are archived:

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

5.5.2 RETENTION PERIOD FOR ARCHIVE

TunTrust retains all documentation relating to certificate requests 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

Archive protections ensure that only authorized trusted access is able to make operations without modifying integrity, authenticity and confidentiality of the data.

5.5.4 ARCHIVE BACKUP PROCEDURES

No stipulation.

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.

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
No stipulation.

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 the CA'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

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

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

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

5.8 CA OR RA TERMINATION

In case of termination of CA operations for any reason whatsoever, 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:

- Revoke all certificates that are still un-revoked or un-expired at the end of the ninety (90)-day,
- Notice period without seeking Subscriber's consent.
- Give timely notice of revocation to each affected Subscriber.
- Make reasonable arrangements to preserve its records according to 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 that are either (i) used as Root CA Key Pairs or (ii) Key Pairs generated for a subordinate CA that is not the operator of the Root CA or an Affiliate of the Root CA, 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 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 stipulation.

6.1.1.3 SUBSCRIBER KEY PAIR GENERATION

TunTrust rejects a certificate request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

As regards to TLS/SSL certificates, Applicants are solely responsible for the generation of the private keys used in their Certificate Requests. TunTrust does not provide SSL key generation, escrow, recovery or backup facilities.

In 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 in an immediately suspended Certificate once generated,
- 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.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

In case of SSL Certificate, subscribers generate Key Pairs and submit the Public Key to TunTrust in a CSR as part of the certificate request process. The Subscriber's signature on the request is authenticated prior to issuing the Certificate.

In 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.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

TunTrust ensures that its Public Keys are delivered to Relying Parties in such a way as to prevent substitution attacks. 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).

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 and uses reasonable techniques to validate the suitability of Public Keys presented by Subscribers. Known weak keys are tested for and rejected at the point of submission. TunTrust references the Baseline Requirements Section 6.1.6 on quality checking.

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

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;
* Certificates for Subordinate CAs and Cross Certificates; and
* Certificates for OCSP Response verification.

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

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). Once the issuing CA is operable, signing operations can be authorized by a single RA operator.

- Subscriber keys: The subscriber has single-person control of the subscriber keys.

6.2.3 PRIVATE KEY ESCROW

TunTrust does not escrow Private Keys for any reason.

6.2.4 PRIVATE KEY BACKUP

For business continuity TunTrust backs up Root and Subordinate Private Keys under the same multi-person control as the original Private Key. TunTrust does not backup Subscriber Private Keys.

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

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

TunTrust ensures that Hardware Security Modules that have been activated are not left unattended or otherwise available to unauthorized access. During the time a TunTrust CA's Hardware Security Module is on-line and operational, it is only used to sign Certificates and CRL/OCSPs from an authenticated RA. When a CA is no longer operational, Private Keys are removed from the Hardware Security Module.

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. In cases when this initialization procedure fails, TunTrust will physically destroy the device to remove the ability to extract any private key.

Subscriber keys: TunTrust does not generate private keys for SSL certificates.

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

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

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

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

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

TunTrust complies with the Baseline Requirements with respect to the maximum Validity Period.

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. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. The cryptographic hardware is held under two-person control as explained in Section 5.2.2. 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 cryptographic module.

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.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

TunTrust CAs activation data are only held by TunTrust personnel in trusted roles.

6.5 COMPUTER SECURITY CONTROLS

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

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.

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

In order to make its environment more secure and to keep it on a state-of-the-art security level, TunTrust operates 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 control processes consist of change control data entries that are processed, logged and tracked for any non-security-related changes to CA systems, equipment and software. Change requests require the approval of a committee.

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

All hardware and software are shipped under standard conditions with controls in place to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering. 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 has mechanisms in place to control and monitor the security-related configurations of its CA systems. Change control processes consist of change control data entries that are processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls. In this manner, TunTrust verifies whether a major change to the system has been properly evaluated for risk mitigation and authorized by management.

6.6.3 LIFE CYCLE SECURITY CONTROLS

No Stipulation.

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 all unused network ports and services are disabled. All firewall configurations and changes thereto are documented, authorized and implemented in accordance with change management procedures.

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

6.8 TIME-STAMPING

All TunTrust CA components are regularly synchronized with a reliable time service. TunTrust CA uses a GPS 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

7.1.1   VERSION NUMBER(S)

All TunTrust CAs Certificates are 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 present document.

7.1.3   ALGORITHM OBJECT IDENTIFIERS

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

7.1.4   NAME FORMS

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. TunTrust does not issue a certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.

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

Certificate policy object identifiers are used as per RFC 3739. The OIDs used by TunTrust are listed in Section 1.2.

7.1.7   USAGE OF POLICY CONSTRAINTS EXTENSION

Usage of Policy Constraints extension is supported as per RFC 5280.

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

7.1.8   POLICY QUALIFIERS SYNTAX AND SEMANTICS

No stipulation.

7.1.9   PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

No stipulation.

7.1.9.1 TUNTRUST CERTIFICATION AUTHORITIES – CERTIFICATES PROFILES

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

7.1.9.2 TUNTRUST END-ENTITY – CERTIFICATES PROFILES

TunTrust end-entity certificate profiles description is available as in the naming and profile document.

7.2 CRL PROFILE

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

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 certificate profiles description is available as in the naming and profile (published in repository http://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 http://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; and

C. 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 CAB Baseline Requirements (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.

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);
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;
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; and
6. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Assessor's relationship to assessed entity.

8.3   ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

TunTrust has selected an auditor/assessor who is completely independent from TunTrust.

8.4 TOPICS COVERED BY ASSESSMENT

The audit meets the requirements of the audit schemes highlighted in Section 8 under which the assessment is being made. These requirements may vary as audit schemes are updated. An audit scheme is applicable to TunTrust in the year following the adoption of the updated scheme.

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

The audit results of processes that are audited according to the ETSI standard are communicated officially to TunTrust by the auditing body.

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

8.7 SELF-AUDITS

During the period in which TunTrust issues Certificates, TunTrust monitors adherence to this CP/CPS and the CAB/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

TunTrust provides a price list for certification and registration services on the website www.tuntrust.tn.

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 their website www.tuntrust.tn or made available upon request.

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

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

9.1.2 CERTIFICATE ACCESS FEES

TunTrust may charge a reasonable fee for access to its certificate databases.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

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

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE
TunTrust encourages customers, Subscribers, End-Entities, Relying Parties, and all other entities to maintain adequate insurance to protect against errors and omissions, professional liability, and general liability. TunTrust currently maintains commercially reasonable insurance.

9.2.2 OTHER ASSETS

No Stipulation.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

No Stipulation.

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 staff including operators 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 8.0.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

The following are not considered confidential:

1. Certificates;

2. Certificate revocation;

3. Certificate status; and

4. TunTrust repositories and their contents.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

TunTrust protects and secures confidential information from disclosure.

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. 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.

9.4.2 INFORMATION NOT DEEMED PRIVATE

Private information does not include Certificates, CRLs, or their contents.

9.4.3 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.

9.4.4 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. TunTrust will only use private information after obtaining the subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate.

9.4.5 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

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

9.4.6 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

No Stipulation.

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 these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

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

1. **Right to Use Domain Name:** That, at the time of issuance, TunTrust (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in TunTrust's Certificate Policy and/or Certification Practice Statement;

2. **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 TunTrust's Certificate Policy and/or Certification Practice Statement;

3. **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 TunTrust's Certificate Policy and/or Certification Practice Statement;

4. **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 TunTrust's Certificate Policy and/or Certification Practice Statement;

5. **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 TunTrust's Certificate Policy and/or Certification Practice Statement;

6. **Subscriber Agreement:** That, if TunTrust and Subscriber are not Affiliated, the Subscriber and TunTrust are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if TunTrust and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;

7. **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

8. **Revocation:** That TunTrust will revoke the Certificate for any of the reasons specified in these Requirements.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

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

TunTrust's agreement with the CRA may contain additional representations.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

TunTrust requires, as part of the Subscriber Agreement, that the Applicant make 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 the 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. TunTrust use an electronic or "click-through" Agreement provided that TunTrust has determined that such agreements are legally enforceable. 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, so 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 stipulation.

9.7 DISCLAIMERS OF WARRANTIES

To the extent permitted by applicable law, this CP/CPS, the Certificate Holder Agreement, the Relying Party Agreement, the Issuing CA Agreement, the Registration Authority Agreement and any other contractual documentation 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 be 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 documentation.

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 replace 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, customers, 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

Changes to this CP/CPS are indicated by appropriate numbering.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

Updates, amendments, and new version 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 a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each such Certificate. 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, Tunisia.

9.15 COMPLIANCE WITH APPLICABLE LAW

TunTrust complies with applicable laws of Tunisia.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

This CP/CPS and the applicable Subscriber Terms and Conditions 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 Terms and Conditions, 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 CLAUSE

If any provision of this CP/CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CP/CPS will be interpreted in such manner as to effect the original intention of the parties.

Each and every provision of this CP/CPS that provides for a limitation of liability is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)

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.