

| | | |
|---|---|--|
|  <p>Agence Nationale de Certification Electronique</p> | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 1 / 85 CL: PU |
|---|---|--|

Agence Nationale de Certification Electronique

TunTrust PKI

Certificate Policy / Certification Practice Statement

| | Author | Validated by | Approved by |
|----------|-------------------------------|--------------------------------|--------------------------------|
| Entity : | TunTrust | TunTrust Board of Directors | TunTrust Board of Directors |
| Date : | August 3 rd , 2020 | August 21 st , 2020 | August 24 th , 2020 |

Table of Contents

| | | |
|------|---|----|
| 1 | INTRODUCTION | 5 |
| 1.1 | Overview..... | 5 |
| 1.2 | Document Name and identification | 5 |
| 1.3 | PKI Participants..... | 6 |
| 1.4 | Certificate Usage | 8 |
| 1.5 | Policy Administration | 8 |
| 1.6 | Definitions and Acronyms | 9 |
| 2 | Publication and Repository Responsibilities | 16 |
| 2.1 | Repositories..... | 16 |
| 2.2 | Publication of Certification Information..... | 17 |
| 2.3 | Time or Frequency of Publication | 17 |
| 2.4 | Access controls on repositories..... | 17 |
| 3 | Identification and Authentication | 18 |
| 3.1 | Naming | 18 |
| 3.2 | Initial Identity Validation | 18 |
| 3.3 | Identification and authentication for re-key requests | 25 |
| 3.4 | Identification and authentication for revocation request..... | 25 |
| 4 | Certificate Life-Cycle Operational Requirements..... | 25 |
| 4.1 | Certificate application | 26 |
| 4.2 | Certificate Application Processing..... | 27 |
| 4.3 | Certificate Issuance | 28 |
| 4.4 | Certificate Acceptance..... | 28 |
| 4.5 | Key pair and Certificate usage..... | 29 |
| 4.6 | Certificate renewal | 30 |
| 4.7 | Certificate Re-Key | 30 |
| 4.8 | Certificate Modification..... | 31 |
| 4.9 | Certificate Revocation and suspension | 31 |
| 4.10 | Certificate Status Services | 36 |
| 4.11 | End of Subscription..... | 37 |
| 4.12 | Key Escrow and recovery..... | 37 |
| 5 | Facility, Management, and operational controls | 37 |

| | | |
|-----|--|----|
| 5.1 | Physical controls | 38 |
| 5.2 | Procedural Controls | 40 |
| 5.3 | Personnel controls..... | 42 |
| 5.4 | Audit Logging Procedures..... | 43 |
| 5.5 | Records archival..... | 46 |
| 5.6 | Key changeover | 47 |
| 5.7 | Compromise and disaster recovery..... | 47 |
| 5.8 | CA or RA Termination | 50 |
| 6 | Technical Security Controls | 50 |
| 6.1 | Key pair generation and installation | 50 |
| 6.2 | Private Key Protection and Cryptographic Module Engineering Controls | 52 |
| 6.3 | Other aspects of key pair management | 55 |
| 6.4 | Activation data | 55 |
| 6.5 | Computer security controls | 56 |
| 6.6 | Life cycle technical controls..... | 56 |
| 6.7 | Network security controls | 57 |
| 6.8 | Time-Stamping..... | 58 |
| 7 | Certificate profile..... | 58 |
| 7.1 | Certificate Profile..... | 58 |
| 7.2 | CRL profile..... | 62 |
| 7.3 | OCSP profile..... | 63 |
| 8 | Compliance Audit and Other Assessments | 63 |
| 8.1 | Frequency or circumstances of assessment..... | 63 |
| 8.2 | Identity/qualifications of assessor..... | 63 |
| 8.3 | Assessor's relationship to assessed entity..... | 64 |
| 8.4 | Topics covered by assessment | 64 |
| 8.5 | Actions taken as a result of deficiency | 64 |
| 8.6 | Communication of results | 64 |
| 8.7 | Self-Audits..... | 65 |
| 9 | Other Business and Legal Matters..... | 65 |
| 9.1 | Fees..... | 65 |
| 9.2 | Financial responsibility | 66 |

| | | |
|---|--|----|
| 9.3 | Confidentiality of business information | 66 |
| 9.4 | Privacy of personal information | 67 |
| 9.5 | Intellectual property rights..... | 68 |
| 9.6 | Representations and warranties | 68 |
| 9.7 | Disclaimers of warranties | 71 |
| 9.8 | Limitations of Liability | 71 |
| 9.9 | Indemnities | 71 |
| 9.10 | Term and termination | 72 |
| 9.11 | Individual notices and communications with participants..... | 73 |
| 9.12 | Amendments | 73 |
| 9.13 | Dispute resolution provisions..... | 73 |
| 9.14 | Governing law..... | 73 |
| 9.15 | Compliance with applicable law | 73 |
| 9.16 | Miscellaneous provisions | 74 |
| 9.17 | Other provisions | 75 |
| Appendix A: TunTrust CA Certificate Profiles | | 76 |
| Appendix B : TunTrust PKI End-entity profiles | | 80 |
| Appendix C : Profiles of the CRL of TunTrust CAs..... | | 82 |
| Appendix D : OCSP Profile Description..... | | 84 |

| | | |
|---|--|---|
|  <p>Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 5 / 85 CL: PU</p> |
|---|--|---|

1 INTRODUCTION

1.1 OVERVIEW

The Agence Nationale de Certification Electronique was founded in accordance with Law no. 2000-83 of 9 August 2000 governing electronic exchanges and commerce in Tunisia. The Agence Nationale de Certification Electronique is a government-owned Certificate Authority (CA) and will be referred to in the remainder of this document with its trademark name "TunTrust".

In this document, the words "TunTrust" and "TunTrust CA" and "TunTrust PKI" are used interchangeably and include the TunTrust Root CAs and Issuing CAs of the Agence Nationale de Certification Electronique.

Referred as Certificate Policy and Certification Practice Statement (CP/CPS), this document has been prepared in compliance with the guide book of "IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" for the purpose of describing how TunTrust executes its operations during providing OV SSL (Organization Validated SSL) certificates to domain names restricted by the ".tn" top-level domain for Tunisia and owned by entities operating under the Tunisian Jurisdiction.

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

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

This CP/CPS also determines practice responsibilities and obligations of TunTrust, applicants, subscribers and relying parties that use or rely on Certificates issued by TunTrust.

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CP/CPS is divided into nine parts that cover the security controls and practices and procedures for Certificate services operated by TunTrust. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement "Not applicable" or "No stipulation" along with a brief explanation of the reason.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the CP/CPS followed by TunTrust while providing OV SSL certification services and was approved for publication by the TunTrust Board of Directors. This CP/CPS document is disclosed to the public at <https://www.tuntrust.tn/repository>.

Note: The OID of TunTrust is joint-iso-itu-t(2) country(16) tn(788) public-sector(1) public-sector-enterprises(2) tuntrust(7). The OID of the present document is: 2.16.788.1.2.7.1.1

| | | |
|---|---|--|
|  Agence Nationale de Certification Electronique | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 6 / 85 CL: PU |
|---|---|--|

Revisions of this document have been made as follows:

| Version | Date | Comment | Changes |
|---------|-------------------|---|--|
| 00 | 19 November 2018 | Draft | The whole document |
| 01 | 12 April 2019 | The first CP/CPS document for public | The whole document |
| 02 | 30 April 2019 | The second version of the CP/CPS | Appendix A, B and C |
| 03 | 20 September 2019 | The third version of the CP/CPS | Sections 1.3, 1.4.2, 1.5, 1.6, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2.1, 4.3.1, 4.4.1, 4.9, 4.10.2, 4.12.2, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 6.1, 6.2, 6.3, 6.4, 6.5, 6.5.2, 6.6, 6.7, 7.1, 7.2.1, 7.3.2, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 9, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.9, 9.11, 9.12, 9.14, 9.15 and 9.16 |
| 04 | 02 October 2019 | The fourth version of the CP/CPS | Sections 1.3.1, 4.2.1, 4.9.3, 4.10.2, 5.4.4, 5.5.1, 5.5.2, 5.5.3, 6.7.2, 7.1.2, 7.1.4 and 7.2.2 |
| 04.1 | 26 May 2020 | Complying with the CA/B Forum SC23, SC24, SC25 & SC27 ballots | Sections 1.6.1, 3.2.2.4, 3.2.2.4.4, 3.2.2.4.18, 3.2.2.4.19, 3.2.2.6, 3.2.2.8, 4.2.2, 4.9.10 and 6.1.5. |
| 04.2 | 24 August 2020 | Complying with the CA/B Forum SC31 and SC33 ballots | Sections 1.6.1, 3.2.2.4.13, 3.2.2.4.20, 3.2.2.8, 4.9.1, 4.9.10, 6.1.1, 6.1.1.3, 6.1.5, 6.3.2, 7.1.2.4, 7.1.3.1, 7.1.3.2, 7.1.4.1, 7.1.6.4, 7.2.2, 7.3, 7.3.2, 8.6, 9.6.3 and Appendix C |

1.3 PKI PARTICIPANTS

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

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

1.3.1 CERTIFICATION AUTHORITY (CA)

TunTrust CA provides OV SSL certification services in accordance with this CP/CPS. As a CA, TunTrust performs functions associated with Public Key operations, including receiving Certificate requests, issuing, and revoking OV SSL Certificates, and maintaining, issuing, and publishing CRLs and OCSP responses.

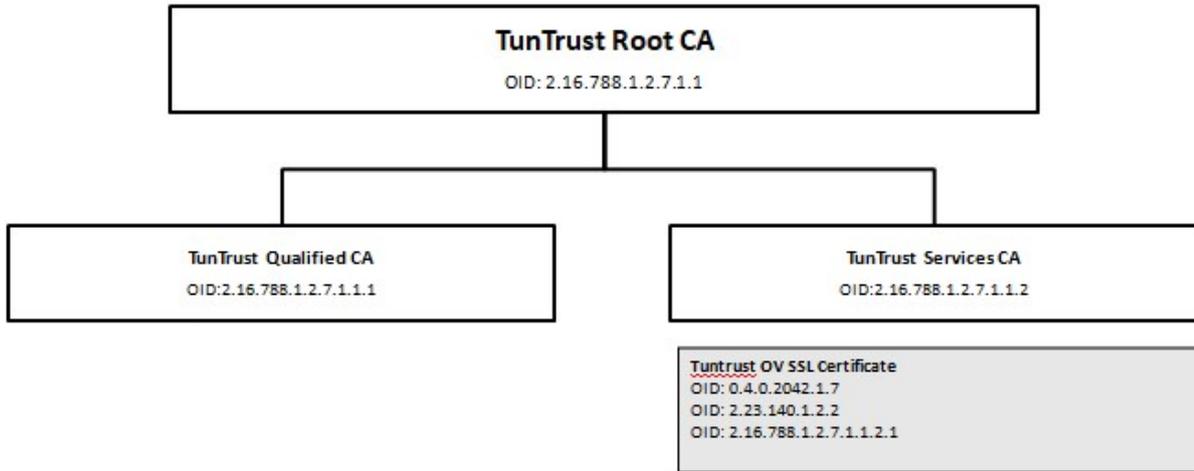
The TunTrust PKI consists of a two-level CA hierarchy:

- **TunTrust Root CA:** root-signing all TunTrust issuing CAs and kept offline.
- **TunTrust Services CA:** This issuing CA is restricted to only issue OV SSL certificates to domain names under “.tn” top-level domain and owned by entities operating under the Tunisian Jurisdiction.

| | | |
|---|--|---|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 7 / 85 CL: PU</p> |
|---|--|---|

- **TunTrust Qualified CA:** This issuing CA is technically constrained to prevent issuance of SSL certificates.

TunTrust does not have any third party Subordinate CAs. Certificate profiles of TunTrust PKI are detailed in Appendix A.



1.3.2 REGISTRATION AUTHORITIES

TunTrust does not delegate the execution of Section 3.2 requirement to a Delegated Third Party. TunTrust operates an internal Registration Authority located in the same infrastructure as its CA offerings, referred to in this document as TunTrust RA, where all registration procedures are directly executed by TunTrust personnel as described in Section 3.2.

TunTrust personnel involved in the issuance of OV SSL certificates must meet and follow the requirements set out in Sections 4.2 and 5.3.

TunTrust RA manages and performs the following roles and responsibilities:

- Identifying and authenticating Applicants for Certificates,
- Accepting, evaluating, approving or rejecting the registration of Certificate applications,
- Using authorized documents or sources of information to evaluate and authenticate an Applicant’s application,
- Initiating the process to revoke a Certificate from the TunTrust CA,
- Archiving of the registration files (electronic and / or paper).

1.3.3 SUBSCRIBERS

Subscribers are legal entities under the Tunisian Jurisdiction who apply for OV SSL Certificates from TunTrust CA and agree to be bound by the relevant Subscriber Agreement. In this document, a subscriber who has registered, but not yet received, a certificate is referred to as an Applicant.

1.3.4 RELYING PARTIES

A Relying party is any natural person or legal entity that relies on a Valid OV SSL Certificate issued by TunTrust CA. Relying Parties are responsible for verifying the validity of the Certificates.

| | | |
|---|--|---|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 8 / 85 CL: PU</p> |
|---|--|---|

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

1.3.5 CERTIFICATE MANAGERS

As part of this CP/CPS, a Certificate Manager is a natural person who is either Applicant, employed by Applicant, or an authorized agent who has express authority to represent Applicant and is responsible for the use of the certificate (and associated private key).

Certificate Managers must meet the conditions and obligations that are set in this CP/CPS and in the Subscriber Agreement. The Certificate is attached to the Subscriber and not to the Certificate Manager. In case of change of Certificate Manager, the Subscriber shall report it to TunTrust and appoint a successor.

1.3.6 OTHER PARTICIPANTS

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

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USAGE

OV SSL Certificates are used to secure online communication and transactions where the risks of data compromise and fraud exist. The OV SSL Certificate allows the end entity to prove its identity to other participants and maintaining the integrity of the transaction.

At all times, Subscribers are required to use Certificates in accordance with this CP/CPS and all applicable laws and regulations.

1.4.2 PROHIBITED CERTIFICATE USES

Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Any usage of the Certificate inconsistent with these extensions is not authorized.

Certificates issued under this CP/CPS may not be used (i) for any application requiring fail safe performance such as (a) air traffic control systems, (b) aircraft navigation systems, (c) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) where prohibited by law.

OV SSL 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

| | | |
|---|--|---|
|  <p>Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 9 / 85 CL: PU</p> |
|---|--|---|

The organization administering the CP/CPS is TunTrust. Its Board of Directors acts as the Certificate Policy Authority. The Board of Directors is composed of the senior management of TunTrust. The TunTrust Board of Directors is the highest level management body with final authority and responsibility for:

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

1.5.2 CONTACT PERSON

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

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

Certificate Problem Reports can be submitted via email to: revoke@tuntrust.tn

1.5.3 PERSON DETERMINING CP/CPS SUITABILITY FOR THE POLICY

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

1.5.4 CP/CPS APPROVAL PROCEDURE

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

1.6 DEFINITIONS AND ACRONYMS

1.6.1 DEFINITIONS

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

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the

| | | |
|---|---|---|
|  <p>Agence Nationale de Certification Electronique</p> | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 10 / 85 CL: PU |
|---|---|---|

Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate request.

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

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

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

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

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

Authorization Domain Name: The 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 (https), 25 (smtp), 22 (ssh).

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

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

CAA: From RFC 8659 (<http://tools.ietf.org/html/rfc8659>): “The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify 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 mis-issue.”

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

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

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

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 11 / 85 CL: PU |
|---|---|---|

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

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

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

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

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

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

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

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

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

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

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

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

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

DNS CAA Phone Contact: The phone number defined in Section A.1.2.

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

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

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

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 12 / 85 CL: PU |
|---|---|---|

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

Domain 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 assignees).

Expiry Date: The “Not After” date in a Certificate that defines the end of a Certificate’s validity period.

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

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

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

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

Individual: A natural person.

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

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

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

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

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 13 / 85 CL: PU</p> |
|---|--|--|

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

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

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

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

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

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

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

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

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

Parent Company: A company that Controls a Subsidiary Company.

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

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

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

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

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

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

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

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the

| | | |
|---|--|--|
|  <p>Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 14 / 85 CL: PU</p> |
|---|--|--|

Certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

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

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

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

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

Request Token: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request. The Request Token SHALL incorporate the key used in the certificate request. A Request Token MAY include a timestamp to indicate when it was created. A Request Token MAY include other information to ensure its uniqueness. A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation. The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

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

- (i) a hash of the public key; or
- (ii) a hash of the Subject Public Key Info [X.509]; or
- (iii) a hash of a PKCS#10 CSR.

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

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

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

The script outputs:

```
201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f
```

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

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

| | | |
|---|---|---|
|  <p>Agence Nationale de Certification Electronique</p> | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 15 / 85 CL: PU |
|---|---|---|

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.

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

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

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

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

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

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

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

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

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

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

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

Test Certificate: This is no longer used in the Baseline Requirements.

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

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

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

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

| | | |
|---|---|---|
|  <p>Agence Nationale de Certification Electronique</p> | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 16 / 85 CL: PU |
|---|---|---|

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

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

Wildcard Certificate: A Certificate containing 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

| | |
|--------|--|
| CA | Certification Authority |
| CAA | Certification Authority Authorization |
| ccTLD | Country Code Top-Level Domain |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSP | Certification Service Provider |
| DBA | Doing Business As |
| DNS | Domain Name System |
| 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 |
| NIST | (US Government) National Institute of Standards and Technology |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| PKI | Public Key Infrastructure |
| 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 makes the following available on its public repository at <https://www.tuntrust.tn/repository>:

- TunTrust CP/CPS;

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 17 / 85 CL: PU |
|---|---|---|

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

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

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

2.2 PUBLICATION OF CERTIFICATION INFORMATION

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

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

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:

- Valid Certificate: <https://validovssl.tuntrust.tn/>
- Revoked Certificate: <https://revokedovssl.tuntrust.tn/>
- Expired Certificate: <https://expiredovssl.tuntrust.tn/>

Prior to issuing SSL Certificates, TunTrust checks for CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued as specified in RFC 6844 as per Section 3.2.2.8. TunTrust's CAA issuer domain is "tuntrust.tn."

2.3 TIME OR FREQUENCY OF PUBLICATION

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

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

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

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

2.4 ACCESS CONTROLS ON REPOSITORIES

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 18 / 85 CL: PU</p> |
|---|--|--|

Read only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

The Subscriber is described in the Certificate by a Distinguished Name pursuant to the X.501 standard.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

Any fully qualified domain name (FQDN) which is embedded into a Certificate either as a DN component, or as a dnsName subjectAltName must conform to the standard semantics for DNS names described in RFC 1034. All DNS names embedded into an OV SSL Certificate issued by TunTrust is restricted by the “.tn” top-level domain for Tunisia and owned by entities operating under the Tunisian Jurisdiction.

Organizational names must be validated to be syntactically identical to an entry in the Tunisian National Registry of Enterprises (Registre National des Entreprises) as was used to validate the certificate request.

If the combination of names or the organization name by itself exceeds 64 characters, TunTrust abbreviates parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit; provided that TunTrust checks this field in accordance with section 3.2.2.10 and a Relying Party will not be misled into thinking that they are dealing with a different organization.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

TunTrust does not issue anonymous or pseudonymous Certificates.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

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

3.1.5 UNIQUENESS OF NAMES

The full combination of the Subject Attributes (DN) is unique within the boundaries defined by this CP/CPS and conforms to all applicable X.500 standards for the uniqueness of names. The SerialNumber attribute guarantees the uniqueness of the DN in the Certificate.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

TunTrust will issue certificates including trademarks only if the trademark is registered in the Tunisian National Register of Enterprises (Registre National des Entreprises). TunTrust will not issue certificates with trademarks that are not documented in the National Register of Enterprises.

3.2 INITIAL IDENTITY VALIDATION

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 19 / 85 CL: PU</p> |
|---|--|--|

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

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

The Applicant 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 OV SSL 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.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

TunTrust issues OV SSL Certificates for public and private organizations under the Tunisian Jurisdiction and having a domain name under the ".tn" top-level domain.

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

3.2.2.1 IDENTITY

TunTrust verifies the existence and identity of the organization using the following methods:

- For Ministries and administrative public enterprises: TunTrust will obtain an excerpt from Official Gazette of Tunisia that proves the legal existence of the entity. Other information such as the address of the entity and the identity of the assigned responsible of the entity are verified based on other legal documents and official correspondences with the requesting agency or a superior government entity.
- For non-administrative public enterprises and private entities: TunTrust will obtain a recent extract from the Tunisian National Register of Enterprises that is not older than 03 months. The register extract includes at a minimum the legal name, legal address, tax identification number, first name and last name of the legal representative.

Alternatively, TunTrust may verify the address, the phone number or email address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, Tunisia Yellow Pages or other form of identification that the CA determines to be reliable.

In order to validate the relationship of a physical person requesting an OV SSL certificate with the organization, the following official documents are required:

- 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 organization.
- A copy of the identity evidence (identity card, passport or Tunisia residency card) of the Certificate Manager.

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:

- A recent extract from the Tunisian National Register of Enterprises not older than 3 months;

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 20 / 85 CL: PU</p> |
|---|--|--|

- Communication with a government entity responsible for the management of such DBAs or tradenames.

The registered DBA/tradename in official document must match the claimed DBA/tradename exactly.

3.2.2.3 VERIFICATION OF COUNTRY

TunTrust verifies that the organization is under the Tunisian jurisdiction. The country field is always set to Tunisia ISO format country code "TN". TunTrust does not issue SSL certificates to organizations that are not under the Tunisian Jurisdiction.

3.2.2.4 VALIDATION OF DOMAIN AUTHORIZATION OR CONTROL

TunTrust confirms that prior to issuance, TunTrust has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below. TunTrust does not issue certificates with a FQDN that contain "onion" as the rightmost label.

TunTrust maintains a record of which domain validation method, including relevant Baseline Requirements version number that was used to validate every domain.

3.2.2.4.1 VALIDATING THE APPLICANT AS A DOMAIN CONTACT

TunTrust does not use this method.

3.2.2.4.2 EMAIL, FAX, SMS, OR POSTAL MAIL 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 (domain name registrant contact, administrative contact or technical contact) listed in WHOIS records of the Tunisian ICANN Accredited Registrar for the ".tn" top-level internet domain <https://whois.ati.tn>. This email provides a confirmation link with a Random Value that the Applicant must follow to confirm control over the domain name. 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.

TunTrust does not use Fax, SMS, or postal mail for Domain Validation.

3.2.2.4.3 PHONE CONTACT WITH DOMAIN CONTACT

TunTrust does not use this method.

3.2.2.4.4 CONSTRUCTED EMAIL TO DOMAIN CONTACT

TunTrust confirms the Applicant's control over the FQDN or Wildcard Domain names by:

1. sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name,
2. including a Random Value in the email, and

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 21 / 85 CL: PU</p> |
|---|--|--|

3. receiving a confirming response utilizing the Random Value.

This email provides a confirmation link with a Random Value that the Applicant must follow to confirm control over the domain name.

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.

3.2.2.4.5 DOMAIN AUTHORIZATION DOCUMENT

TunTrust does not use this method.

3.2.2.4.6 AGREED-UPON CHANGE TO WEBSITE

TunTrust does not use this method.

3.2.2.4.7 DNS CHANGE

TunTrust does not use this method.

3.2.2.4.8 IP ADDRESS

TunTrust does not use this method.

3.2.2.4.9 TEST CERTIFICATE

TunTrust does not use this method.

3.2.2.4.10 TLS USING A RANDOM NUMBER

TunTrust does not use this method.

3.2.2.4.11 ANY OTHER METHOD

TunTrust does not use any other method.

3.2.2.4.12 VALIDATING APPLICANT AS A DOMAIN CONTACT

TunTrust does not use this method.

3.2.2.4.13 EMAIL TO DNS CAA CONTACT

TunTrust may confirm the Applicant's control over the FQDN by sending a Random Value via email to a DNS CAA Email Contact. This email provides a confirmation link with a Random Value that the Applicant must follow to confirm control over the domain name.

In this case, the relevant CAA Resource Record Set is found using the search algorithm defined in RFC 8659 Section 3.

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 22 / 85 CL: PU</p> |
|---|--|--|

Each email may confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email may be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated.

The Random Value is unique in each email. TunTrust may re-send the email in its entirety, including the reuse of the Random Value, provided that its 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.

3.2.2.4.14 EMAIL TO DNS TXT CONTACT

TunTrust may confirm the Applicant's control over the FQDN by sending a Random Value via email. This email provides a confirmation link with a Random Value that the Applicant must follow to confirm control over the domain name.

In this case, the Random Value is sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN.

Each email may confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email may be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated.

The Random Value is unique in each email. TunTrust may re-send the email in its entirety, including the reuse of the Random Value, provided that its 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.

3.2.2.4.15 PHONE CONTACT WITH DOMAIN CONTACT

TunTrust does not use this method.

3.2.2.4.16 PHONE CONTACT WITH DNS TXT RECORD PHONE CONTACT

TunTrust does not use this method.

3.2.2.4.17 PHONE CONTACT WITH DNS TXT RECORD PHONE CONTACT

TunTrust does not use this method.

3.2.2.4.18 AGREED-UPON CHANGE TO WEBSITE V2

TunTrust does not use this method.

3.2.2.4.19 AGREED-UPON CHANGE TO WEBSITE - ACME

TunTrust does not use this method.

3.2.2.4.20 TLS USING ALPN

TunTrust does not use this method.

3.2.2.5 AUTHENTICATION FOR AN IP ADDRESS

TunTrust does not issue certificates with IP addresses.

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 23 / 85 CL: PU |
|---|---|---|

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” under the “.tn” domain (e.g. tn, com.tn, ens.tn, fin.tn, gov.tn, ind.tn, intl.tn, nat.tn, net.tn, org.tn, info.tn, perso.tn, tourism.tn, edunet.tn, rrnt.tn, rns.tn, rnu.tn, mincom.tn, agrinet.tn, defense.tn, turen.tn).

If a wildcard would fall within the label immediately to the left of a registry-controlled¹ or public suffix, the TunTrust issuing CAs refuse issuance unless the Applicant proves its rightful control of the entire Domain Namespace.

3.2.2.7 DATA SOURCE ACCURACY

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

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

- The age of the information provided,
- The frequency of updates to the information source,
- The data provider and purpose of the data collection,
- The public accessibility of the data availability, and
- The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA RECORDS

Prior to issuing SSL Certificates, TunTrust checks for CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued as specified in RFC 8659. TunTrust's CAA issuer domain is "TunTrust.tn.". The following cases do not allow TunTrust to authorize the issuance of the certificate:

- The CAA DNS field is present, it contains an "issue" or "issuewild" tag and does not list TunTrust.tn as an authorized Certificate Authority;
- The CAA DNS field is present, it is designated as "critical" and the tag used is not supported by the CA (it is not an "issue" or "issuewild" tag);
- The zone is validly DNSSEC-signed and our DNS query times out.

If any of these cases are encountered, the certificate request is automatically blocked and the applicant is notified by email of the need to update the associated DNS records. TunTrust:

¹ Determination of what is “registry-controlled” versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a “public suffix list” such as <http://publicsuffix.org/> (PSL), and to retrieve a fresh copy regularly. If using the PSL, a CA SHOULD consult the "ICANN DOMAINS" section only, not the "PRIVATE DOMAINS" section. The PSL is updated regularly to contain new gTLDs delegated by ICANN, which are listed in the "ICANN DOMAINS" section. A CA is not prohibited from issuing a Wildcard Certificate to the Registrant of an entire gTLD, provided that control of the entire namespace is demonstrated in an appropriate way.

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 24 / 85 CL: PU |
|---|---|---|

- Caches CAA records for reuse for up to 8 hours
- Supports the issue and issuewild CAA tags
- Processes but does not act on iodef property tag (i.e., TunTrust does not dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s))
- Does not support any additional property tags.

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; and
- The lookup has been retried at least once; and
- The domain's zone does not have a DNSSEC validation chain to the ICANN root

3.2.2.9 VERIFICATION AGAINST THE DENIED LIST

TunTrust CA maintains an internal database of all previously revoked SSL Certificates and previously rejected Certificate requests due to suspected phishing or other fraudulent usage or concerns. TunTrust uses this information to identify subsequent suspicious certificate requests. If a new request for a previously denied SSL Certificate is made, the application will be flagged and brought to the attention of management to complete further internal verification and final decision.

3.2.2.10 VERIFICATION AGAINST HIGH RISK CERTIFICATE REQUEST

TunTrust develops, maintains, and implements documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified by doing the following:

- TunTrust maintains a list of prior high risk requests specifying current high risk Domain Names. This list is used by TunTrust to identify potential risks.
- TunTrust also uses an automated Domain name permutation engine for detecting potential typosquatting and phishing threat.

Application with potential High Risk will be flagged and brought to the attention of management to complete further internal verification and final decision.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

TunTrust does not issue OV SSL certificates to natural persons. However, as part of the certificate application process, TunTrust will verify the identity of the Certificate Manager and the legal representative of the organization as detailed in Section 3.2.2.1.

The Certificate Manager is either the Legal Representative of the entity or a natural person formally designated by the Legal Representative. The designation of a Certificate Manager is performed simultaneously with the submission of the OV SSL Certificate Application Form.

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 25 / 85 CL: PU</p> |
|---|--|--|

As mentioned in Section 4.1.2, the Certificate Application Form is signed by : (i) the Legal Representative to mandate the future Certificate Manager and (ii) the future Certificate Manager to accept this role and the Subscriber Agreement.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

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

3.2.5 VALIDATION OF AUTHORITY

This step is performed simultaneously with the validation of the identity of the Legal Representative and of the Certificate Manager. As mentioned in Section 3.2.3 , the certificate application form is signed by the legal representative of the entity and the certificate manager and each of them must provide a copy of his or her ID. Signatures of the Legal Representative and Certificate Manager must be a legally valid and contain an enforceable seal or handwritten signature or be a legally valid and enforceable electronic signature.

In addition, TunTrust uses a Reliable Method of Communication derived from the verification process described in section 3.2.2.1 to establish the authenticity of the certificate request directly with the Applicant Legal Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that TunTrust deems appropriate.

3.2.6 CRITERIA FOR INTEROPERATION

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

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

Not Applicable. TunTrust does not support rekey.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

Not Applicable. TunTrust does not support re-key.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

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

TunTrust may also perform revocation on behalf of Subscribers in accordance with the requirements of the applicable Subscriber Agreement. Examples of reasons for revocation include a breach of the Subscriber Agreement or non-payment of applicable fees.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 26 / 85 CL: PU</p> |
|---|--|--|

4.1 CERTIFICATE APPLICATION

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

OV SSL certificates applications can only be submitted by Applicant under the Tunisian Jurisdiction. Applicants must comply with provisions set within the registration forms and processes, this CP/CPS and the Subscriber Agreement.

TunTrust maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. TunTrust uses this information to identify 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.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

TunTrust makes available to Applicants all required Application forms as well as all applicable Subscriber Agreements: (i) on its public repository at <https://www.tuntrust.tn/repository>, (ii) by email to tuntrust@tuntrust.tn, (iii) and within its headquarters (see Section 1.5.2).

Prior to the issuance of a Certificate, TunTrust obtains a dully filled and signed Application Form that falls into five parts as described hereafter:

- Part 1 : Applicant details including legal name, tax identification number, a telephone number, fax number, email address, and postal delivery address,
- Part 2 : Legal Representative details including full name, ID Number, telephone number and email address
- Part 3 : Certificate Manager details including full name, ID Number, telephone number and email address
- Part 4 : Certificate type; Certificate Validity, FQDN Names to embed into the SSL Certificate
- Part 5 : Signature of the Legal Representative and the Certificate Manager by which they confirm their acceptance and compliance with the Subscriber Agreement

The Applicant commits to providing a current, genuine and complete certificate request and all evidence requested by TunTrust. The paper Application, with the Applicant wet seal and handwritten signatures of the Applicant's legal representative and the Certificate Manager, must be physically submitted to a TunTrust RA. Applicant may submit electronic Application Form with the digital signature of the Applicant Legal Representative and the Certificate Manager. The digital signatures of Legal Representative and Certificate Manager must be compliant to the Tunisian Law related to digital signature.

The Applicant generates the key pair by itself and creates a Certificate Signing Request (CSR) as to prove that the private key belongs to itself and sends this to TunTrust RA from email address used to verify domain control or provides it to TunTrust RA operator on a hardware device (CD, USB Token). The Applicant is responsible for taking all required measures for protecting confidentiality and integrity of its private key.

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 27 / 85 CL: PU</p> |
|---|--|--|

TunTrust's responsibility is to verify and to validate the information supplied. This will be done in compliance with the practices stated in this CP/CPS and by strictly following the TunTrust registration procedures and the applicable national laws.

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

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

Applications for OV SSL Certificates shall be submitted by the legal representative of the organization who owns the Domain Name.

OV SSL Certificate application includes the following:

- Order Form including the Subscriber Agreement as described in Section 4.1.
- Certificate Manager Documents proving the legal existence of the Applicant (Section 3.2.2)
- Copy of the ID of the legal representative (identity card, passport or Tunisia residency card)
- Copy of the ID of the Certificate Manager (identity card, passport or Tunisia residency card)
- The Certificate Signing Request (CSR) that includes at least one Fully-Qualified Domain Name to be included in the Certificate's SubjectAltName extension.

The following verification tasks are performed by TunTrust's RA:

- Validation of the identity and the legal existence of the Applicant (Section 3.2.2) : The Applicant must be a legal entity under the Tunisian Jurisdiction;
- Validation of the identity of the legal representative and the Certificate Manager (section 3.2.2);
- Validation of domain control (section 3.2.2.4);
- Assurance that the certificate request does not fall into high risk or blacklisted certificate requests (Section 3.2.2.9 and Section 3.2.2.10);
- Verification of CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued (Section 3.2.2.8).

TunTrust does not re-use previous validation information. Each certificate application must go through all validation functions described in section 3.2. End-user Certificate validity is less than 825 days as specified in Section 6.3.2

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

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

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 28 / 85 CL: PU</p> |
|---|--|--|

TunTrust rejects any certificate application that TunTrust cannot verify. TunTrust does not issue Certificates for domain names that are not under the “.tn” top-level domain. TunTrust does not issue certificates containing Internal Names.

TunTrust, in its sole discretion, may reject a Certificate Application, 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 proceeds to the Certificate issuance process.

Certificate issuance by TunTrust CAs requires a Tuntrust RA operator in Trusted Role authorized by TunTrust to deliberately issue a direct command in order for TunTrust CAs to perform a certificate signing operation. Each issuance is logged with the identity of the TunTrust RA operator issuing the certificate and the action logged in the CA audit log.

TunTrust CAs uses an automated issuance process that integrates pre-issuance linting tools, kept up-to-date, which can check a tbsCertificate (To Be Signed Certificate - the certificate complete except for the signature) for a large number of standards violations (BRs, RFCs etc.). Certificate issuance is held up for manual review if a linting error or warning is found. The linting error is flagged and brought to the attention of management to complete further internal verification and final decision on the certificate issuance.

Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the certificate is stored in a database and sent to the Subscriber.

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

The Applicant will be notified that the Certificate is issued via the Certificate Manager email address that was supplied by the Subscriber during the enrollment process and will be provided with appropriate instructions on how to obtain the Certificate. If the Certificate is presented to the Subscriber immediately, special notification may not be necessary.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 29 / 85 CL: PU</p> |
|---|--|--|

A Subscriber that accepts a Certificate warrants to TunTrust, that all information supplied in connection with the application process and all information included in the Certificate issued to them is true, complete, and not misleading.

Without limitation to the generality of the foregoing, the use of a Certificate signifies acceptance by that Subscriber of this CP/CPS and Subscriber Agreement (as the same may, from time to time, be amended or supplemented) by which they irrevocably agree to be bound.

If the subscriber is not satisfied with the details contained within the certificate, he or she must email assistance@tuntrust.tn explaining why the certificate is not being accepted. This communication must take place within 30 days of issuance.

Certificates are considered accepted 30 days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

Refer to Section 2.1.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Other than Certificate Transparency publication, TunTrust does not notify other entities of certificate issuance.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

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

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

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

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

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

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

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

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

| | | |
|---|---|---|
|  <p>Agence Nationale de Certification Electronique</p> | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 30 / 85 CL: PU |
|---|---|---|

- 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 OCSP or CRL Checks.

4.6 CERTIFICATE RENEWAL

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

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.2 WHO MAY REQUEST RENEWAL

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable. Certificate renewal is not supported by TunTrust.

4.7 CERTIFICATE RE-KEY

Certificate re-key means the issuance of a new certificate with a new public key, but with the same subject identity information. TunTrust does not support re-key.

4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

Not Applicable. TunTrust does not support re-key.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

Not Applicable. TunTrust does not support re-key.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUEST

Not Applicable. TunTrust does not support re-key.

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 31 / 85 CL: PU</p> |
|---|--|--|

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable. TunTrust does not support re-key.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Not Applicable. TunTrust does not support re-key.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

Not Applicable. TunTrust does not support re-key.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable. TunTrust does not support re-key.

4.8 CERTIFICATE MODIFICATION

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

4.8.1 CIRCUMSTANCES FOR CERTIFICATE MODIFICATION

Not Applicable. TunTrust does not support Certificate modification.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

Not Applicable. TunTrust does not support Certificate modification.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

Not Applicable. TunTrust does not support Certificate modification.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable. TunTrust does not support Certificate modification.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

Not Applicable. TunTrust does not support Certificate modification.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

Not Applicable. TunTrust does not support Certificate modification.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable. TunTrust does not support Certificate modification.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 32 / 85 CL: PU</p> |
|---|--|--|

4.9.1 CIRCUMSTANCES OF REVOCATION

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

4.9.1.1 REASONS FOR REVOKING A SUBSCRIBER CERTIFICATE

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

1. The Subscriber requests in writing that TunTrust revoke the Certificate;
2. The Subscriber notifies TunTrust that the original Certificate request was not authorized and does not retroactively grant authorization;
3. TunTrust obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. TunTrust is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see <https://wiki.debian.org/SSLkeys>); or
5. TunTrust obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

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

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. TunTrust obtains evidence that the Certificate was misused;
3. TunTrust is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
4. TunTrust is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. TunTrust is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. TunTrust is made aware of a material change in the information contained in the Certificate;
7. TunTrust is made aware that the Certificate was not issued in accordance with the Baseline Requirements or the CA's Certificate Policy or Certification Practice Statement;
8. TunTrust determines or is made aware that any of the information appearing in the Certificate is inaccurate;
9. 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;
10. Revocation is required by this CP/CPS; or
11. TunTrust is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.1.2 REASONS FOR REVOKING A SUBORDINATE CA CERTIFICATE

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 33 / 85 CL: PU</p> |
|---|--|--|

TunTrust does not have any third party Subordinate CAs. The only CAs that TunTrust operates are the ones listed in section 1.3.1.

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

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies TunTrust Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. TunTrust Issuing CA 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;
4. TunTrust Issuing CA obtains evidence that the Certificate was misused;
5. TunTrust Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the CA/B Forum Baseline Requirements or the applicable CP/CPS;
6. TunTrust Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. TunTrust Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. TunTrust Issuing CA's or Subordinate CA's right to issue Certificates under the CA/B Forum Baseline Requirements expires or is revoked or terminated, unless TunTrust Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by TunTrust Issuing CA's Certificate Policy and/or Certification Practice Statement.

4.9.2 WHO CAN REQUEST REVOCATION

TunTrust accepts authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or its appropriately authorized Certificate Manager.

Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports to notify TunTrust of a suspected reasonable cause to revoke the Certificate. Problem Reports shall be submitted to the Contact Person specified in Section 1.5.2. TunTrust may also at its own discretion revoke Certificates.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

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

- Using TunTrust online service available at <https://www.tuntrust.tn/fr/content/revocation-certificat>. In this case, the Subscriber is required to provide :
 - The revocation challenge (shared secret) that was communicated to the Subscriber upon delivery of the certificate and
 - The FQDN listed in the certificate.

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 34 / 85 CL: PU</p> |
|---|--|--|

- The email address used for domain control validation. A notification will be sent to this email upon certificate revocation.
- Physical presence before a TunTrust RA operator: Either the Certificate Manager or the Legal Representative of the Subscriber must be physically present at the headquarters (Section 1.5.2) of TunTrust and request the revocation of a Certificate in writing after providing a valid ID.
- For Certificate Problem Report submitted by third parties to the Contact Person specified in Section 1.5.2, TunTrust personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
 - The nature of the alleged problem,
 - The evidence provided in support of the request,
 - The urgency of the request,
 - The number of reports received about a particular certificate or website,
 - The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered),
 - and Tunisian National Legislation

4.9.4 REVOCATION REQUEST GRACE PERIOD

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

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

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

After reviewing the facts and circumstances, TunTrust will work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which TunTrust will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation does not exceed the time frame set forth in Section 4.9.1.1.

4.9.6 REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

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

4.9.7 CRL ISSUANCE FREQUENCY

- For the status of TunTrust CA Certificates:

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

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 35 / 85 CL: PU</p> |
|---|--|--|

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

4.9.8 MAXIMUM LATENCY FOR CRLS

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

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

TunTrust supports OCSF responses in addition to CRLs. Response times are generally no longer than 5 seconds under normal network operating conditions.

TunTrust OCSF responses conform to RFC6960 and/or RFC5019. OCSF responses are signed by an OCSF Responder whose Certificate is signed by TunTrust CAs that issued the Certificate whose revocation status is being checked. OCSF signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

The OCSF responder operated by TunTrust supports the HTTP GET method as described in RFC 6960 and/or RFC 5019.

The validity interval of an OCSF response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

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

- For the status of Subscriber Certificates:

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

- For the status of Issuing CA Certificates:

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

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

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

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 36 / 85 CL: PU</p> |
|---|--|--|

1. "assigned" if a Certificate with that serial number has been issued by TunTrust Issuing CA, using any current or previous key associated with that CA subject; or
2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by (a) TunTrust Issuing CA; or (b) a Precertificate Signing Certificate [RFC6962] associated with TunTrust Issuing CA; or
3. "unused" if neither of the previous conditions are met.

TunTrust requires OCSP requests to contain the following data:

- Protocol version
- Service request
- Target Certificate identifier

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

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

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

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

4.9.13 CIRCUMSTANCES FOR SUSPENSION

No suspension of Certificates is performed by TunTrust.

4.9.14 WHO CAN REQUEST SUSPENSION

No suspension of Certificates is performed by TunTrust.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

No suspension of Certificates is performed by TunTrust.

4.9.16 LIMITS ON SUSPENSION PERIOD

No suspension of Certificates is performed by TunTrust.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

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

4.10.2 SERVICE AVAILABILITY

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

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 37 / 85 CL: PU</p> |
|---|--|--|

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

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

4.10.3 OPERATIONAL FEATURES

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

4.11 END OF SUBSCRIPTION

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

4.12 KEY ESCROW AND RECOVERY

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

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

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

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

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

TunTrust does not provide session key encapsulation and recovery.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

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

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to TunTrust by law.

The Certificate Management Process includes:

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 38 / 85 CL: PU |
|---|---|---|

1. Physical security and environmental controls;
2. System integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. Network security and firewall management, including port restrictions and IP address filtering;
4. User management, separate trusted-role assignments, education, awareness, and training; and
5. Logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

TunTrust performs an annual Risk Assessment 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 Processes;
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.

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

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

5.1 PHYSICAL CONTROLS

5.1.1 SITE LOCATION AND CONSTRUCTION

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

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

5.1.2 PHYSICAL ACCESS

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

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 39 / 85 CL: PU |
|---|---|---|

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

All critical CA operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software. Such systems are physically separated from the organization's other systems so that only authorized employees of the CA can access them.

The secure parts of TunTrust CA hosting facilities are protected using physical access controls with biometric scanners or card access systems making them accessible only to appropriately authorized individuals. CA operational facilities are physically locked and alarmed when unoccupied.

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

5.1.3 POWER AND AIR CONDITIONING

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

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

5.1.4 WATER EXPOSURES

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

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

5.1.5 FIRE PREVENTION AND PROTECTION

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

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

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

5.1.6 MEDIA STORAGE

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

5.1.7 WASTE DISPOSAL

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 40 / 85 CL: PU</p> |
|---|--|--|

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

5.1.8 OFF-SITE BACKUP

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

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

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 internal auditors.

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

The following roles are deemed to be trusted roles:

| | |
|-----------------------|---|
| Validation Specialist | Employees responsible for routine certification services such as customer services, document control, processes relating to Subscriber Certificate registration, generation and revocation. They are also responsible for interacting with Applicants and Subscribers, managing the Certificate request queue and completing the Certificate approval checklist as identity vetting items are successfully completed. A person to whom this role is assigned can be a shareholder of CA private keys activation data. |
| System Administrator | The System Administrator is responsible for the installation and configuration of PKI components (CA, RA, ...).This administrator is also responsible for keeping PKI systems updated with software patches and other maintenance needed for system stability and recoverability. A person to whom this role is assigned can be a shareholder of CA private keys activation data. |
| System Operator | The System Operator is responsible for the installation and configuration of the system hardware, including servers and different components of the Front End / Internal Support System. The System Administrator is also responsible for keeping systems updated with software patches and other maintenance needed for system stability and recoverability. A person to whom this role is assigned can be a shareholder of CA private keys |

| | | |
|---|---|---|
|  <p>Agence Nationale de Certification Electronique</p> | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 41 / 85 CL: PU |
|---|---|---|

| | |
|---------------------------------------|---|
| | activation data. |
| Application Administrator | The Application Administrator is a trusted role. This administrator is responsible for the installation, configuration and operations of the applications related to TunTrust. |
| Physical and Logical Security Officer | <p>The Physical and Logical Security Officer is a trusted role. This role 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).</p> <p>A person to whom this role is assigned can be a shareholder of CA private keys activation data.</p> |
| Auditor | The Auditor is authorized to view archives and audit logs. The auditor is also responsible for overseeing internal compliance to determine if TunTrust is operating in accordance with this CP/CPS. This includes acting as internal auditor in TunTrust key ceremonies. A person to whom this role is assigned cannot be a shareholder of CA private keys activation data. |
| Key/Ceremony Manager | The Key/Ceremony Manager is responsible of conducting the key ceremonies. |
| Shareholders | Holders of secret shares needed to operate TunTrust CA private keys. |

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

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

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

- (a) Key generation of Root CA = 3 of 6
- (b) Signing key activation of Root CA = 3 of 6
- (c) Private key backup and restore of Root CA = 3 of 6
- (d) Key generation of Issuing CA = 2 of 6
- (e) Signing key activation of Issuing CA = 2 of 6
- (f) Private key backup and restore of Issuing CA = 3 of 6

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 42 / 85 CL: PU |
|---|---|---|

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

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

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

To accomplish this separation of duties, TunTrust specifically designates individuals to trusted roles.

TunTrust’s systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

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

Prior to the engagement of any TunTrust employee in the Certificate Management Process, , TunTrust verifies the identity and trustworthiness of such person who must be a TunTrust permanent employee. All TunTrust personnel must sign the internal security charter.

Trusted roles and responsibilities, as specified in Section 5.2.1 are documented in job descriptions. TunTrust personnel have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

5.3.2 BACKGROUND CHECK PROCEDURES

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

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

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

5.3.3 TRAINING REQUIREMENTS

TunTrust provides suitable training to all staff before they take on a Trusted Role should they not already have the complete skill-set required for that role. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.

TunTrust provides all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including this CP/CPS), common threats to the information verification process (including phishing and social engineering), and the CA/B Forum requirements. TunTrust maintains records of such training and ensures that personnel

| | | |
|---|--|--|
|  <p>Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 43 / 85 CL: PU</p> |
|---|--|--|

entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

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

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

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

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

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

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

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

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

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

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

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

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

TunTrust does not assign Trusted Roles to external Contractors.

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

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

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

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

5.4 AUDIT LOGGING PROCEDURES

5.4.1 TYPES OF EVENTS RECORDED

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 44 / 85 CL: PU |
|---|---|---|

TunTrust 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.

- CA key lifecycle management events, including:
 - a. Key generation, backup, storage, recovery, archival, and destruction; and
 - b. Cryptographic device lifecycle management events.
 - c. CA and Subscriber Certificate lifecycle management events, including: Certificate requests and revocation;
 - d. All verification activities stipulated in this CP/CPS;
 - e. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
 - f. Acceptance and rejection of Certificate requests;
 - g. Issuance of Certificates; and
 - h. Generation of Certificate Revocation Lists and OCSP entries.

- 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:

- Date and time of entry ;
- the identity of the entity and/or operator that caused the event; and
- Description of the entry.

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

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

5.4.2 FREQUENCY OF PROCESSING LOG

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

A human review of the logging processes is also performed on application and system logs at least once every 30 days to validate the integrity of logging processes and ensure that monitoring, logging, alerting, and log integrity-verification functions are operating properly.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

TunTrust retains any audit logs generated for at least 20 years as per Tunisia national law. TunTrust makes these audit logs available to its Qualified Auditor upon request.

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 45 / 85 CL: PU</p> |
|---|--|--|

5.4.4 PROTECTION OF AUDIT LOG

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

All automated log events are recorded real-time to a secured central logging services in order to prevent log shrinkage or unexpected alteration. Logs stored offsite reside in facilities which have protections at least equivalent to the TunTrust originating systems.

Off-site logs are digitally signed to make tampering of the logs evident. The encryption key used for signing audit logs is not used for any other purpose. Offsite logs are verified periodically to ensure that their integrity has been maintained.

5.4.5 AUDIT LOG BACKUP PROCEDURES

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

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

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

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

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

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

5.4.8 VULNERABILITY ASSESSMENTS

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

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

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

Additionally, TunTrust performs annual risk assessments that:

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 46 / 85 CL: PU |
|---|---|---|

- 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;
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that TunTrust has in place to counter such threats.

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF RECORDS ARCHIVED

TunTrust backs up application, network and system data including :

- Registration information of Subscribers (signed subscriber agreements, IDs of Subscribers, signed Certificate request Forms, proof of legal existence of the organization, etc.),
- Configuration files of TunTrust CA systems,
- All audit logs listed in section 5.4.1,
- Certificate lifecycle information,
- All versions of the CP/CPS and internal documents, including security policies and procedures,
- Ceremony scripts of TunTrust CA key events.

5.5.2 RETENTION PERIOD FOR ARCHIVE

TunTrust retains all documentation relating to Certificate applications and the verification thereof, and all Certificates and revocation thereof, for at least 20 years after any Certificate based on that documentation ceases to be valid. Event logs specified in Section 5.4 are archived for twenty years after their generation.

5.5.3 PROTECTION OF ARCHIVE

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

5.5.4 ARCHIVE BACKUP PROCEDURES

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

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

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

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

Archive information is collected internally by TunTrust.

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 47 / 85 CL: PU</p> |
|---|--|--|

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

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

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

5.6 KEY CHANGEOVER

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

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

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 48 / 85 CL: PU |
|---|---|---|

9. Regular testing of contingency plans.

10. TunTrust's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes

11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;

12. What constitutes an acceptable system outage and recovery time

13. How frequently backup copies of essential business information and software are taken;

14. The distance of recovery facilities to TunTrust 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 RECOVERY PROCEDURES IF COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

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

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

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

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

- Collect all information related to the incident (and if the event is ongoing, ensure that all data are being captured and recorded);
- Begin investigating the incident and determine the degree and scope;
- 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);
- Contact law enforcement, and other interested parties and activate any other appropriate additional security measures;
- Monitor system, continue the investigation, ensure that all data is still being recorded as evidence and make a forensic copy of data collected;
- Isolate, contain and stabilize the system, applying any possible short-term fixes needed to return the system to a normal operating state;

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 49 / 85 CL: PU |
|---|---|---|

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

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

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

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

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

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

5.7.5 MISS-ISSUANCE HANDLING PROCEDURES

In miss-issuance cases, TunTrust will immediately cease issuance from the affected part of TunTrust PKI until the source of the problem has been diagnosed and identified.

Once the problem is diagnosed, TunTrust will put in place at minimum temporary or manual procedures to prevent the problem from re-occurring until a fully automated fix is applied in a reasonable amount of time. TunTrust will restart Certificate issuance after approval of the TunTrust Certificate Policy Authority .

As per Section 4.9.1.1, TunTrust will scan corpus of issued certificates and revoke all certificates found with the same issue.

TunTrust will report the miss-issuance incident to its auditor and to the browser root certificate programs of which TunTrust is a member at the earliest possible date post-incident. The incident report should cover at least the following topics:

- How TunTrust CA first became aware of the problem (e.g. via a problem report submitted to TunTrust, a notification from the browser root certificate programs of which TunTrust is a member, or internal self-audit), and the time and date.
- A timeline of the actions TunTrust CA took in response. A timeline is a date-and-time-stamped sequence of all relevant events. This may include events before the incident was reported, such as when a particular requirement became applicable, or a document changed, or a bug was introduced, or an audit was done.
- The date and time TunTrust has stopped issuing certificates with the problem.
- A summary of the problematic Certificates. For each problem: number of Certificates, and the date the first and last Certificates with that problem were issued.
- The complete certificate data for the problematic certificates.
- Explanation about how and why the mistakes were made or bugs introduced, and how they avoided detection until now.

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 50 / 85 CL: PU</p> |
|---|--|--|

- List of steps TunTrust CA is taking to resolve the situation and ensure such issuance will not be repeated in the future, accompanied with a timeline of when TunTrust CA expects to accomplish these things and restart Certificate issuance.

5.8 CA OR RA TERMINATION

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

- Provide subscribers of valid certificates, the operators of the browser root certificate programs and the CA/B Forum with ninety (90) days notice of its intention to cease acting as a CA,
- Revoke all certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking subscriber’s consent,
- Destroy all private keys,
- Give timely notice of revocation to each affected Subscriber.

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

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

6.1.1.1 CA KEY PAIR GENERATION

For the Root CA Key Pairs, TunTrust performs the following controls:

1. prepares and follows a Key Generation Script,
2. has a Qualified Auditor witness the CA Key Pair generation process or records a video of the entire 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 section 5.1 of this CP/CPS;
2. generates the CA Key Pair using personnel in trusted roles under the principles of multiple person control and split knowledge as disclosed in section 6.2.1 of this CP/CPS;
3. generates the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in section 6.2.2 of this CP/CPS;
4. logs its CA Key Pair generation activities and log all physical access during the key ceremony as disclosed in section 5.4 ; and
5. maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in Section 6.2 of this CP/CPS and its Key Generation Script.

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 51 / 85 CL: PU |
|---|---|---|

6.1.1.2 RA KEY PAIR GENERATION

No key pair generation is made for TunTrust RA.

6.1.1.3 SUBSCRIBER KEY PAIR GENERATION

TunTrust does not generate a Key Pair on behalf of a Subscriber and does not accept a certificate request using a Key Pair previously generated by TunTrust.

TunTrust rejects a Certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Sections 6.1.5 and/or 6.1.6
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. TunTrust is aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise;
4. TunTrust has previously been made aware that the Subscriber's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;
5. TunTrust is aware of a demonstrated or proven method to easily compute the Subscriber's Private Key based on the Public Key (such as a Debian weak key, see <http://wiki.debian.org/SSLkeys>).

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

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 operations.

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

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

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.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

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

The browser root certificate programs of which TunTrust is a member will also embed Root Certificate Public Keys into root stores and operating systems.

6.1.5 KEY SIZES

TunTrust uses RSA key pairs and it:

- Ensures that the modulus size, when encoded, is at least 2048 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8.

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

| | | |
|---|---|---|
|  Agence Nationale de Certification Electronique | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 52 / 85 CL: PU |
|---|---|---|

6.1.5.1 ROOT CA CERTIFICATES

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

6.1.5.2 SUBORDINATE CA CERTIFICATES

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

6.1.5.3 SUBSCRIBER CERTIFICATES

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

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

TunTrust uses a HSM device that conforms to FIPS 186 2 and provides random number generation and onboard generation of up to 4096 bit RSA Public Key. The value of the public exponent is equal to : 65537.

TunTrust uses CA software that performs quality checks on generated keys for both RSA and ECC algorithms and also performs regular internal audits against randomly selected samples of Subscriber Certificates per section 8.7.

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

Private Keys corresponding to Root Certificates are not used to sign Certificates except in the following cases:

- Self-signed Certificates to represent the Root CA itself;
- Certificates for Subordinate CAs and Cross Certificates; and
- Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates).

The key usage extension is set in accordance with the certificate profile requirements specified in section 7.1.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 53 / 85 CL: PU</p> |
|---|--|--|

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

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

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

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

- Root CA keys : The HSM used for CA keys meets FIPS 140-2 level 3 requirements.
- Issuing CAs keys: The HSM used for CA keys meets FIPS 140-2 level 3 requirements. Subscriber keys (SSL Certificate) : The Subscriber is fully responsible for his/her private keys.

A check of the integrity and tests of functionalities of HSMs are done by personnel in trusted roles upon delivery of the HSMs to TunTrust facility. In addition to that, TunTrust maintains controls to provide reasonable assurance that physical access to the HSMs is limited to authorized personnel in trusted roles.

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

In all instances, CA private keys are generated in a physically secure environment within cryptographic modules that are validated to FIPS 140-2 Level-3. CA Certificate signing keys are only used within this secure environment. Access to the modules within the TunTrust environment, including the private keys, is restricted by the use of token/smart cards and associated pass phrases. These smartcards and pass phrases are allocated among multiple Shareholders in trusted roles. Such allocation ensures that no one member of TunTrust personnel in Trusted Roles holds total control over any component of the system. The hardware security modules are always stored in a physically secure environment and are subject to security controls throughout their lifecycle.

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

- Root CA keys : Root CA keys can only be accessed on the physical and on the logical level by adhering to '3 out of 6' control, meaning that 3 of the 6 persons are present.
- Issuing CAs keys : Management access to these keys is only possible using '4-eye' principle (2 out of 6).
- Subscriber keys: 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

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

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 54 / 85 CL: PU</p> |
|---|--|--|

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

6.2.5 PRIVATE KEY ARCHIVAL

TunTrust does not archive Subscriber Private Keys.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

TunTrust CA Private Keys are generated, activated and stored in Hardware Security Modules. Private Keys are exported from the HSM only for backup purposes. Private keys are transferred between HSMs according to manufacturers' specifications, and only leave the originating device in encrypted form.

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

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

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

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

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

The following list shows how private keys are activated:

- Root CA keys: The Root CA keys are activated with three user keys (physical) and three user PINs (knowledge).
- Issuing CA keys: The Issuing CA keys are activated with two user keys (physical) and two user PINs (knowledge).
- Subscriber keys: Subscribers are solely responsible for protecting Private Keys in accordance with the obligations that are presented in Subscriber Agreement.

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

TunTrust deactivates access to its CA Private Keys and stores its cryptographic modules in a secure safe when not in use. TunTrust never leaves its HSM devices in an active unlocked or unattended state.

The method specified in Section 6.2.8 is operated for re-activation of private key.

6.2.10 METHOD OF DESTROYING PRIVATE KEY

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

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

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 55 / 85 CL: PU |
|---|---|---|

TunTrust does not generate private keys for Subscriber 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

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

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

The Validity Periods of Certificates issued by TunTrust are as follows:

- The TunTrust Root CA is valid for 25 years from April 26th, 2019 to April 26th, 2044.
- The Validity Periods of the issuing CAs Certificates are 20 years from April 26th, 2019 to April 26th, 2039.
- Effective August 27th, 2020, the end-user Certificates (SSL OV Certificates) have a Validity period not greater than 398 days.

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

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

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

6.4.2 ACTIVATION DATA PROTECTION

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

Repeated attempts to wrongly enter PIN data will cause the activation devices to lock out, and new device issuance to be required.

Subscribers are solely responsible for protecting their private keys activation credentials (PIN, password) and not share them with anyone else.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

TunTrust CA activation data are only held by TunTrust personnel in trusted roles as specified in section 5.2.1.

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 56 / 85 CL: PU</p> |
|---|--|--|

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

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

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

6.5.2 COMPUTER SECURITY RATING

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

As described in section 5.4.8, the systems themselves and the services running on the systems are subject to thorough reviews and testing (including penetration testing). TunTrust operates also a vulnerability management process which includes monitoring of supplier security alerts.

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

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

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

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

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 57 / 85 CL: PU |
|---|---|---|

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

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

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

6.6.2 SECURITY MANAGEMENT CONTROLS

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

6.6.3 LIFE CYCLE SECURITY CONTROLS

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

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

- Remediate the Critical Vulnerability; If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to (1) vulnerabilities with high CVSS scores, starting with the vulnerabilities TunTrust determines are the most critical (such as those with a CVSS score of 10.0) and (2) systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or
- Document the factual basis for the TunTrust determination that the vulnerability does not require remediation because (a) TunTrust disagrees with the NVD rating, (b) the identification is a false positive, (c) the exploit of the vulnerability is prevented by compensating controls or an absence of threats; or (d) other similar reasons.

6.7 NETWORK SECURITY CONTROLS

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

TunTrust maintains the Root CA Systems in a High Security Zone and in an offline state or air-gapped from all other networks. TunTrust Root CA Keys are kept offline and brought on-line only when necessary to sign Certificate Issuing CAs or periodic CRLs or OCSP Certificates.

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 58 / 85 CL: PU</p> |
|---|--|--|

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

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

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

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

6.8 TIME-STAMPING

All TunTrust CA components are regularly synchronized with a reliable time service. TunTrust CA uses a GPS-NTP time source to establish the correct time for:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates; and
- Issuance of Subscriber end entity Certificates.

7 CERTIFICATE PROFILE

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

7.1 CERTIFICATE PROFILE

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

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

7.1.1 VERSION NUMBER(S)

TunTrust CAs issue X.509 version 3 Certificates.

7.1.2 CERTIFICATE CONTENT AND EXTENSIONS; APPLICATION OF RFC 5280

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

7.1.2.1 ROOT CA CERTIFICATE

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 59 / 85 CL: PU</p> |
|---|--|--|

See Appendix A.

7.1.2.2 SUBORDINATE CA CERTIFICATE

See Appendix A.

7.1.2.3 SUBSCRIBER CERTIFICATE

See Appendix B.

7.1.2.4 ALL CERTIFICATES

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

TunTrust does not issue a Certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in section 7.1.2.1, 7.1.2.2, or 7.1.2.3.

TunTrust does not issue a Certificate with:

- a. extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network), unless:
 - i. such value falls within an OID arc for which the Applicant demonstrates ownership, or
 - ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or
- b. semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA (such as including extendedKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.2.5 APPLICATION OF RFC 5280

For purposes of clarification, a Pre-certificate, as described in RFC 6962 – Certificate Transparency, shall not be considered to be a “certificate” subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under the current Baseline Requirements.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

All signing algorithms used by TunTrust are sha256WithRSAEncryption. TunTrust CA does not, and never has, used SHA-1 as a component of any signature algorithm on a certificate.

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

7.1.3.1 SUBJECTPUBLICKEYINFO

TunTrust uses RSA key pairs and it:

- Ensures that the modulus size, when encoded, is at least 2048 bits, and;
- Ensures that the modulus size, in bits, is evenly divisible by 8.

7.1.3.2 SIGNATURE ALGORITHM IDENTIFIER

| | | |
|---|--|--|
|  <p>Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 60 / 85 CL: PU</p> |
|---|--|--|

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

In particular, it applies to all of the following objects and fields:

- The signatureAlgorithm field of a Certificate or Precertificate.
- The signature field of a TBSCertificate (for example, as used by either a Certificate or Precertificate).
- The signatureAlgorithm field of a CertificateList
- The signature field of a TBSCertList
- The signatureAlgorithm field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

When encoded, the `AlgorithmIdentifier` is byte-for-byte identical with the specified hex-encoded bytes: RSASSA-PKCS1-v1_5 with SHA-256: `300d06092a864886f70d01010b0500`.

7.1.4 NAME FORMS

7.1.4.1 NAME ENCODING

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.

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate is byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate is byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

7.1.4.2 SUBJECT INFORMATION – SUBSCRIBER CERTIFICATES

TunTrust Issuing CAs do not include a Domain Name in a Subject attribute except as specified in Section 3.2.2.4 or Section 3.2.2.5.

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

7.1.4.2.1 SUBJECT ALTERNATIVE NAME EXTENSION

The subjectAltName extension contains at least one entry. Each entry is a dNSName containing the Fully-Qualified Domain Name of a server. TunTrust confirms that the Applicant controls the Fully-Qualified Domain Name or has been granted the right to use it by the Domain Name Registrant, as specified in Section 3.2.2.4.

Wildcard FQDNs are permitted in accordance to section 3.2.2.6.

TunTrust does not issue:

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 61 / 85 CL: PU</p> |
|---|--|--|

- certificates with a subjectAlternativeName extension or Subject commonName field containing an IP Address or Internal Name; and
- certificates that have underscore characters (“_”) in dNSName entries.

7.1.4.2.2 SUBJECT DISTINGUISHED NAME FIELDS

See SSL Certificate Profile in Appendix B.

7.1.4.3 SUBJECT INFORMATION – ROOT CERTIFICATES AND SUBORDINATE CA CERTIFICATES

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

7.1.4.3.1 SUBJECT DISTINGUISHED NAME FIELDS

See Root and Subordinate Certificates Profiles in Appendix A.

7.1.5 NAME CONSTRAINTS

The TunTrust Services CA is technically constrained with restrictions to issue SSL Certificate for domain names under the top level domain ".tn" and owned by entities under the Tunisian Jurisdiction. However, all TunTrust CAs are subject for full audit as specified in section 8 of this CP/CPS.

| | |
|---|--|
| <p>TunTrust Services CA X509v3 Name Constraints</p> | <p>Permitted: DNS:tn DirName: C = TN Excluded: IP:0.0.0.0/0.0.0.0 IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0:0</p> |
|---|--|

The TunTrust Qualified CA is constrained to prevent issuance of SSL Certificates.

| | |
|--|--|
| <p>TunTrust Qualified CA X509v3 Extended Key Usage</p> | <p>Extended Key Usage TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin</p> |
|--|--|

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

7.1.6.1 RESERVED CERTIFICATE POLICY IDENTIFIERS

SSL certificates must contain the certificate policy identifier 2.23.140.1.2.2.

7.1.6.2 ROOT CA CERTIFICATES

TunTrust Root CA certificates do not contain any certificatePolicies extension, therefore do not have policy identifiers in them.

7.1.6.3 SUBORDINATE CA CERTIFICATES

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 62 / 85 CL: PU</p> |
|---|--|--|

TunTrust Issuing CAs contain the following policy identifiers (as described in Appendix A):

- TunTrust Services CA: 2.16.788.1.2.7.1.1.2
- TunTrust Qualified CA: 2.16.788.1.2.7.1.1.1

7.1.6.4 SUBSCRIBER CERTIFICATES

The certificate policy identifiers of the Subscriber Certificates are listed in the certificate policies extension as described in Appendix B.

TunTrust Issuing CAs assert that the Certificates it issues containing the specified policy identifiers listed in the certificate policies extension in Appendix B, are managed in accordance with the CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

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

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

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

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

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

7.2 CRL PROFILE

7.2.1 VERSION NUMBER(S)

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

7.2.2 CRL AND CRL ENTRY EXTENSIONS

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

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

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

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

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

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

| | | |
|---|--|--|
|  <p>Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 63 / 85 CL: PU</p> |
|---|--|--|

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.

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

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

7.3.1 VERSION NUMBER

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

7.3.2 OCSP EXTENSIONS

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

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

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

- the applicable laws;
- the requirements of this CP/CPS;
- the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates of the CA/B Forum; and
- the latest versions of the WebTrust Principles And Criteria For Certification Authorities – SSL Baseline With Network Security and the WebTrust Principles And Criteria For Certification Authorities.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

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

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

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 64 / 85 CL: PU |
|---|---|---|

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

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.1 of the CA/B Forum Baseline Requirements);
3. For audits conducted in accordance with the WebTrust standard licensed by WebTrust;
4. For audits conducted in accordance with any one of the ETSI standards accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
5. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function; and
6. Bound by law, government regulation, or professional code of ethics.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4 TOPICS COVERED BY ASSESSMENT

TunTrust undergoes an audit in accordance with the current versions of WebTrust for CAs and WebTrust for CAs SSL Baseline with Network Security. Topics covered in this annual audit include, but are not limited to, the requirements of this CP/CPS, environmental controls, CA key management, and certificate life cycle management.

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

The audit is conducted by a Qualified Auditor, as specified in Section 8.2.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

If the deficiency is deemed so serious, or the time to remediate so long as to call into question the integrity of certificates issued, TunTrust CA will inform the relevant browser root certificate program managers that a serious deficiency in practice has been uncovered, and that they should take such steps as to mitigate the risk to their program's integrity.

8.6 COMMUNICATION OF RESULTS

| | | |
|---|--|--|
|  <p>Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 65 / 85 CL: PU</p> |
|---|--|--|

TunTrust makes the Audit Report publicly available at <https://www.tuntrust.tn/repository>. The results will also be sent to any other appropriate entities that may be entitled by law, regulation, or agreement to receive a copy of the audit results. Such parties include the relevant browser root certificate program managers.

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

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

1. name of the organization being audited;
2. name and address of the organization performing the audit;
3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, that were in-scope of the audit;
4. audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
5. a list of the CA policy documents, with version numbers, referenced during the audit;
6. whether the audit assessed a period of time or a point in time;
7. the start date and end date of the Audit Period, for those that cover a period of time;
8. the point in time date, for those that are for a point in time;
9. the date the report was issued, which will necessarily be after the end date or point in time date.

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

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

8.7 SELF-AUDITS

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

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

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

TunTrust charges fees for issuing of Certificates according to the respective price list published on their website <https://www.tuntrust.tn> or made available upon request.

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 66 / 85 CL: PU</p> |
|---|--|--|

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

9.1.2 CERTIFICATE ACCESS FEES

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

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

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

9.1.4 FEES FOR OTHER SERVICES

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

9.1.5 REFUND POLICY

TunTrust does not refund the fees of Certificates.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

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

9.2.2 OTHER ASSETS

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

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

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

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

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

- Private Keys;
- Activation data used to access Private Keys or to gain access to the CA system;
- Disaster Recovery, and Business Continuity Plans

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 67 / 85 CL: PU</p> |
|---|--|--|

- Any certificate application records and documentation submitted in support of certificate applications, which is not in relation to an issued certificate, whether successful or rejected.
- External or internal audit trail records and reports, which are not required to be openly published.
- Transaction records, financial audit records, and internal records on the operations of TunTrust’s infrastructure, certificate management, services and data.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

The following are not considered confidential:

- Certificates;
- Certificate revocation Lists;
- CP/CPS; and
- any information available in TunTrust repository at <https://www.tuntrust.tn/repository>.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

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

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 PRIVACY PLAN

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

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

9.4.2 INFORMATION TREATED AS PRIVATE

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

9.4.3 INFORMATION NOT DEEMED PRIVATE

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

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

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

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 68 / 85 CL: PU</p> |
|---|--|--|

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

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

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

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

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

9.5 INTELLECTUAL PROPERTY RIGHTS

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

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

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

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA REPRESENTATIONS AND WARRANTIES

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

- The Subscriber that is a party to the Subscriber Agreement
- All Application Software Suppliers with whom TunTrust has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
- All Relying Parties who reasonably rely on a Valid Certificate.

TunTrust represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, TunTrust has complied with the CA/B Forum Baseline Requirements and this CP/CPS in issuing and managing the Certificate. The Certificate Warranties specifically include, but are not limited to, the following:

- **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 this CP/CPS;

| | | |
|---|---|---|
|  | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 69 / 85 CL: PU |
|---|---|---|

- **Authorization for Certificate:** That, at the time of issuance, TunTrust (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
- **Accuracy of Information:** That, at the time of issuance, TunTrust (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
- **No Misleading Information:** That, at the time of issuance, TunTrust (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate’s subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, TunTrust (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2 and 11.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
- **Subscriber Agreement:** That, if TunTrust and the Subscriber are not Affiliated, the Subscriber and TunTrust are parties to a legally valid and enforceable Subscriber Agreement that satisfies the CA/B Forum Baseline Requirements, or, if TunTrust and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
- **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
- **Revocation:** That TunTrust will revoke the Certificate for any of the reasons specified in the CA/B Forum Baseline Requirements.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

TunTrust RA represents that:

- Information provided by TunTrust RA does not contain any false or misleading information, and
- All Certificates requested by TunTrust RA meet the requirements of the applicable CP/CPS.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

TunTrust requires, as part of the Subscriber Agreement, that the Applicant makes the commitments and warranties in this section for the benefit of TunTrust and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, TunTrust obtains, for the express benefit of TunTrust and the Certificate Beneficiaries, the Applicant’s agreement to the Subscriber Agreement with TunTrust CA.

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

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

| | | |
|---|--|--|
|  <p>Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 70 / 85 CL: PU</p> |
|---|--|--|

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:

- **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;
- **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);
- **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
- **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;
- **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.
- **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.
- **Responsiveness:** An obligation to respond to TunTrust’s instructions concerning Key Compromise or Certificate misuse within a specified time period.
- **Acknowledgment and Acceptance:** An acknowledgment and acceptance that TunTrust is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or if revocation is required by the present CP/CPS, or the CA/B Forum Baseline Requirements.

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

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

- Obtained sufficient knowledge on the use of digital Certificates and PKI,
- Studied the applicable limitations on the usage of Certificates and agrees to TunTrust’s limitations on liability related to the use of Certificates,
- Has read, understands, and agrees to this CP/CPS,
- Verified both the TunTrust Certificate and the Certificates in the Certificate chain using the relevant CRL or OCSP,
- Will not use a TunTrust Certificate if the Certificate has expired or been revoked, and
- Will take all reasonable steps to minimize the risk associated with relying on a TunTrust Certificate after considering:
 - applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
 - the intended use of the Certificate as listed in the Certificate or this CP/CPS,

| | | |
|---|--|--|
|  <p>Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 71 / 85 CL: PU</p> |
|---|--|--|

- the data listed in the Certificate,
- 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,
- the Relying Party’s previous course of dealing with the Subscriber,
- the Relying Party’s understanding of trade, including experience with computer-based methods of trade, and
- any other indication of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

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

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

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

9.7 DISCLAIMERS OF WARRANTIES

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

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

9.8 LIMITATIONS OF LIABILITY

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

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

TunTrust is not in any event liable for damages that result from force major events as detailed in section 9.15.5. TunTrust takes commercially reasonable measures to mitigate the effects of force major in due time. Any damages resulting of any delay caused by force major will not be covered by TunTrust.

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

9.9 INDEMNITIES

9.9.1 INDEMNIFICATION BY TUNTRUST

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 72 / 85 CL: PU</p> |
|---|--|--|

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

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

9.9.2 INDEMNIFICATION BY SUBSCRIBERS

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

9.9.3 INDEMNIFICATION BY RELYING PARTIES

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

9.10 TERM AND TERMINATION

9.10.1 TERM

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

9.10.2 TERMINATION

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

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 73 / 85 CL: PU</p> |
|---|--|--|

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

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

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

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

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

9.12.2 NOTIFICATION MECHANISM AND PERIOD

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

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

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

9.13 DISPUTE RESOLUTION PROVISIONS

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

9.14 GOVERNING LAW

This CP/CPS is governed, construed and interpreted in accordance with the laws of Tunisia. This choice of law is made to ensure consistency with TunTrust CA restriction to issue SSL Certificate for entities under the Tunisian jurisdiction. The law of Tunisia applies also to all TunTrust commercial or contractual relationships in which this CP/CPS may apply or quoted implicitly or explicitly in relation to TunTrust products and services where TunTrust acts as a provider, supplier, beneficiary receiver or otherwise.

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

9.15 COMPLIANCE WITH APPLICABLE LAW

| | | |
|---|---|---|
|  Agence Nationale de Certification Electronique | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 74 / 85 CL: PU |
|---|---|---|

TunTrust is subject to all national applicable laws of Tunisia.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

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

9.16.2 ASSIGNMENT

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

9.16.3 SEVERABILITY

In the event of a conflict between the CA/B Forum Baseline Requirements and a Tunisian law, regulation or government order, TunTrust may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in Tunisia.

This applies only to operations or certificate issuances that are subject to that Law. In such event, TunTrust will immediately (and prior to issuing a certificate under the modified requirement) include in this section a detailed reference to the Law requiring a modification of the CA/B Forum Baseline Requirements under this section, and the specific modification to the Baseline Requirements implemented by TunTrust.

TunTrust will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CP/CPS.

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

9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)

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

TunTrust's failure to enforce a provision of this CP/CPS does not waive TunTrust's right to enforce the same provision later, or right to enforce any other provision of this CP/CP.

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.

| | | |
|---|--|--|
|  <p>Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 75 / 85 CL: PU</p> |
|---|--|--|

9.17 OTHER PROVISIONS

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

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 76 / 85 CL: PU</p> |
|---|--|--|

APPENDIX A: TUNTRUST CA CERTIFICATE PROFILES

1. TunTrust Root CA

The following table describes the certificate profile of TunTrust Root CA:

| Fields | Critical | Values |
|---------------------------------|----------|---|
| Version | | 3 (0x2) |
| Serial Number | | 13:02:d5:e2:40:4c:92:46:86:16:67:5d:b4:bb:bb:b2:6b:3e:fc:13 |
| Signature Algorithm | | sha256WithRSAEncryption |
| Issuer | | C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA |
| Validity | | |
| Not Before | | Apr 26 08:57:56 2019 GMT |
| Not After | | Apr 26 08:57:56 2044 GMT |
| Subject | | C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA |
| Subject Public Key Info | | |
| Public Key Algorithm | | rsaEncryption |
| RSA Public Key | | 4096 bit |
| Exponent | | 65537 (0x10001) |
| X509v3 extensions | | |
| X509v3 Subject Key Identifier | | SHA-1 Hash of Subject public key |
| X509v3 Basic Constraints | True | CA: TRUE |
| X509v3 Authority Key Identifier | | Keyid: 06:9A:9B:1F:53:7D:F1:F5:A4:C8:D3:86:3E:A1:73:59:B4:F7:44:21 |
| X509v3 Key Usage | True | Certificate Sign, CRL Sign |
| Signature Algorithm | | sha256WithRSAEncryption |

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 77 / 85 CL: PU</p> |
|---|--|--|

2. TunTrust Qualified CA

The following table describes the certificate profile of TunTrust Qualified CA:

| Fields | Critical | Values |
|---------------------------------|----------|---|
| Version | | 3 (0x2) |
| Serial Number | | 64:0c:48:27:ee:90:3e:af:b4:d7:3d:b2:79:7a:91:af:c9:85:72:7a |
| Signature Algorithm | | sha256WithRSAEncryption |
| Issuer | | C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA |
| Validity | | |
| Not Before | | Apr 26 09:49:02 2019 GMT |
| Not After | | Apr 26 09:49:02 2039 GMT |
| Subject | | C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Qualified CA |
| Subject Public Key Info | | |
| Public Key Algorithm | | rsaEncryption |
| RSA Public Key | | 4096 bit |
| Exponent | | 65537 (0x10001) |
| X509v3 extensions | | |
| Authority Information Access | | CA Issuers - URI:http://www.tuntrust.tn/pub/TnTrustRootCA.crt OCSP - URI:http://va.tuntrust.tn |
| X509v3 Subject Key Identifier | | 28:6C:72:5F:B0:89:10:9C:8E:10:D6:30:96:9E:8F:FC:FB:9F:74:36 |
| X509v3 Basic Constraints | True | CA:TRUE, pathlen:0 |
| X509v3 Authority Key Identifier | | Keyid: 06:9A:9B:1F:53:7D:F1:F5:A4:C8:D3:86:3E:A1:73:59:B4:F7:44:21 |
| X509v3 Certificate Policies | | Policy: 2.16.788.1.2.7.1.1.1 |
| X509 CRL Distribution Points | | URI:http://crl.tuntrust.tn/titrustrootca.crl |
| X509v3 Key Usage | True | Certificate Sign, CRL Sign |
| X509v3 Extended Key Usage | | TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin |
| Signature Algorithm | | sha256WithRSAEncryption |

| | | |
|---|---|---|
|  <p>Agence Nationale de Certification Electronique</p> | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 78 / 85 CL: PU |
|---|---|---|

3. TunTrust Services CA

The following table describes the certificate profile of TunTrust Services CA:

| Fields | Critical | Values |
|---------------------------------|----------|--|
| Version | | 3 (0x2) |
| Serial Number | | 60:1a:7c:2f:60:93:b7:a6:73:da:5f:8c:9c:88:5f:37:a7:58:97:c0 |
| Signature Algorithm | | sha256WithRSAEncryption |
| Issuer | | C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA |
| Validity | | |
| Not Before | | Apr 26 10:23:31 2019 GMT |
| Not After | | Apr 26 10:23:31 2039 GMT |
| Subject | | C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Services CA |
| Subject Public Key Info | | |
| Public Key Algorithm | | rsaEncryption |
| RSA Public Key | | 4096 bit |
| Exponent | | 65537 (0x10001) |
| X509v3 extensions | | |
| X509v3 Name Constraints | True | Permitted: DNS:tn DirName: C = TN Excluded: IP:0.0.0.0/0.0.0.0 IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0 |
| Authority Information Access | | CAIssuers - URI:http://www.tuntrust.tn/pub/TnTrustRootCA.crt OCSP - URI:http://va.tuntrust.tn |
| X509v3 Subject Key Identifier | | 9F:25:17:CE:6F:90:AB:61:2F:C1:47:A9:E0:2F:99:13:5D:FA:23:39 |
| X509v3 Basic Constraints | True | CA: TRUE, pathlen:0 |
| X509v3 Authority Key Identifier | | Keyid: 06:9A:9B:1F:53:7D:F1:F5:A4:C8:D3:86:3E:A1:73:59:B4:F7:44:21 |
| X509v3 Certificate Policies | | Policy: 2.16.788.1.2.7.1.1.2 |
| X509 CRL Distribution Points | | URI:http://crl.tuntrust.tn/tntrustrootca.crl |
| X509v3 Key Usage | True | Certificate Sign, CRL Sign |
| X509v3 Extended Key Usage | | TLS Web Server Authentication, TLS Web Client Authentication |

| | | |
|---|--|--|
|  <p>Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 79 / 85 CL: PU</p> |
|---|--|--|

| | |
|---------------------|-------------------------|
| Signature Algorithm | sha256WithRSAEncryption |
|---------------------|-------------------------|

| | | |
|---|---|---|
|  <p>Agence Nationale de Certification Electronique</p> | TunTrust PKI Certificate Policy / Certification Practice Statement | Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 80 / 85 CL: PU |
|---|---|---|

APPENDIX B : TUNTRUST PKI END-ENTITY PROFILES

The following table provides the description of the fields for TunTrust OVCP SSL Certificates issued under

1. TunTrust Services CA

| Base Profile | Included | Critical | O/M ² | CO ³ | Values |
|---------------------|----------|----------|------------------|-----------------|--|
| Data: | | | | | |
| Version | X | False | M | S | 3 (0x2) |
| Serial Number | X | False | M | FDV | Validated on duplicates |
| Signature Algorithm | X | False | M | S | SHA256 with RSA Encryption |
| Issuer | X | False | M | S | C=TN,O=Agence Nationale de Certification Electronique, CN=TunTrust Services CA |
| Validity | | | | | |
| Not Before | X | False | M | D | Certificate generation process date/time |
| Not After | X | False | M | D | Certificate generation process date/time + 365 days . |
| Subject | | | | | |
| C, countryName | X | False | M | S | TN |
| L, localityName | X | False | M | D | Location in which the company's registered office is established. |
| O, OrganizationName | X | False | M | D | Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA. |
| serialNumber | X | False | M | D | Serial Number as constructed by TunTrust RA |
| CN, commonName | X | False | O | D | FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or unique name of server. |

²O/M: O = Optional, M = Mandatory.

³CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

| Subject Public Key Info: | | | | | |
|---------------------------------|---|-------|---|---|---|
| Public Key Algorithm | X | False | M | S | rsaEncryption |
| RSA Public Key | X | False | M | S | (2048 bit) |
| Modulus (2048 bit) | X | False | M | S | |
| Exponent | X | False | M | S | 65537 (0x10001) |
| X509v3 extensions | | | | | |
| Authority Information Access | X | False | M | S | CA Issuers - URI:http://www.tuntrust.tn/pub/TunTrustService sCA.crt OCSP - URI:http://va.tuntrust.tn |
| X509v3 Subject Key Identifier: | X | False | M | D | This extension identifies the public key being certified. |
| X509v3 Basic Constraints: | X | True | M | S | CA:False |
| X509v3 Authority Key Identifier | X | False | M | S | keyid:9F:25:17:CE:6F:90:AB:61:2F:C1:47:A9:E0:2F: :99:13:5D:FA:23:39 |
| X509v3 Certificate Policies | X | False | M | S | Policy: 2.16.788.1.2.7.1.1.2.1 Policy : 0.4.0.2042.1.7 Policy: 2.23.140.1.2.2 |
| X509v3 CRL Distribution Points | X | False | M | S | URI:http://crl.tuntrust.tn/TunTrustservicesca.crl |
| X506v3 Key Usage | X | True | M | S | Digital Signature, Key Encipherment |
| X509v3 Extended Key Usage | X | False | M | S | TLS Web Client Authentication, TLS Web Server Authentication |
| X509v3 Subject alternative Name | X | False | M | D | DNS: FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or unique name of server. |

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 82 / 85 CL: PU</p> |
|---|--|--|

APPENDIX C : PROFILES OF THE CRL OF TUNTRUST CAS

1. TunTrust Root CA CRL

The following table describes the CRL profile of TunTrust Root CA:

| Field | Value |
|---------------------------------|--|
| Version | 2 (0x1) |
| Signature Algorithm | sha256WithRSAEncryption |
| Issuer | /CN=TunTrust Root CA/O=Agence Nationale de Certification Electronique/C=TN |
| Last Update | CRL generation process date/time. |
| Next Update | CRL generation process date/time + 365 days |
| CRL extensions | |
| X509v3 Authority Key Identifier | 6:9A:9B:1F:53:7D:F1:F5:A4:C8:D3:86:3E:A1:73:59:B4:F7:44:21 |
| X509v3 CRL Number | A monotonically increasing sequence number |
| Revoked Certificates: | |
| Serial Number | Serial number of the revoked certificate |
| Revocation Date | Date and time of the revocation |
| CRL entry extensions: | |
| X509v3 CRL Reason Code | Code of Reason of revocation |
| Signature Algorithm | sha256WithRSAEncryption |

2. TunTrust Qualified CA CRL

The following table describes the CRL profile of TunTrust Qualified CA:

| Field | Value |
|---------------------------------|---|
| Version | 2 (0x1) |
| Signature Algorithm | sha256WithRSAEncryption |
| Issuer | /CN=TunTrust Qualified CA/O=Agence Nationale de Certification Electronique/C=TN |
| Last Update | CRL generation process date/time. |
| Next Update | CRL generation process date/time + 6 days |
| CRL extensions | |
| X509v3 Authority Key Identifier | 28:6C:72:5F:B0:89:10:9C:8E:10:D6:30:96:9E:8F:FC:FB:9F:74:36 |
| X509v3 CRL Number | A monotonically increasing sequence number |
| Revoked Certificates: | |
| Serial Number: | Serial number of the revoked certificate |
| Revocation Date | Date and time of the revocation |
| CRL entry extensions: | |
| X509v3 CRL Reason Code | Code of Reason of revocation |
| Signature Algorithm | sha256WithRSAEncryption |

| | | |
|---|--|--|
|  <p>tuntrust Agence Nationale de Certification Electronique</p> | <p>TunTrust PKI Certificate Policy / Certification Practice Statement</p> | <p>Code : PL/SMI/16 Version : 04.2 Date : 24/08/2020 Page : 83 / 85 CL: PU</p> |
|---|--|--|

3. TunTrust Services CA CRL

The following table describes the CRL profile of TunTrust Services CA:

| Field | Value |
|---------------------------------|--|
| Version | 2 (0x1) |
| Signature Algorithm | sha256WithRSAEncryption |
| Issuer | /CN=TunTrust Services CA/O=Agence Nationale de Certification Electronique/C=TN |
| Last Update | CRL generation process date/time. |
| Next Update | CRL generation process date/time + 6 days |
| CRL extensions | |
| X509v3 Authority Key Identifier | 9F:25:17:CE:6F:90:AB:61:2F:C1:47:A9:E0:2F:99:13:5D:FA:23:39 |
| X509v3 CRL Number | A monotonically increasing sequence number |
| Revoked Certificates: | |
| Serial Number | Serial number of the revoked certificate |
| Revocation Date | Date and time of the revocation |
| CRL entry extensions: | |
| X509v3 CRL Reason Code | Code of Reason of revocation |
| Signature Algorithm | sha256WithRSAEncryption |

APPENDIX D : OCSP PROFILE DESCRIPTION

| Base Profile | Included | Critical | O/M ⁴ | CO ⁵ | Values |
|----------------------|----------|----------|------------------|-----------------|--|
| Version | X | False | | S | Version 3 Value='2' |
| Serial Number | X | False | | FDV | Validated on duplicates |
| Signature Algorithm | | | | | |
| Algorithm | X | False | | S | OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption |
| Signature Value | X | False | | D | Issuing CA Signature |
| Issuer DN | X | | | S | Issuing CA DN |
| Subject DN | X | False | | | |
| commonName | X | | M | D | Name of the validation Authority |
| countryName | X | | M | D | Country in which the organization's registered office is established (ISO3166). |
| OrganizationName | X | | M | D | Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA. |
| Locality | X | | M | D | Locality Name |
| Validity | X | False | | | |
| Not Before | X | | | D | Certificate generation process date/time |
| Not After | X | | | D | Certificate generation process date/time + 730 days |
| subjectPublicKeyInfo | X | False | | | |
| Algorithm | X | | | | Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001) |
| SubjectPublicKey | X | | M | | |
| X509v3 extensions | | | | | |

⁴O/M: O = Optional, M = Mandatory. ⁴

⁵CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

| | | | | | |
|---------------------------------|---|-------|--|---|---|
| X509v3 Authority Key Identifier | X | | | | Authority Key Identifier |
| authorityInfoAccess | X | False | | | |
| Authority Information Access | X | | | | OCSP - URI:http://va.certification.tn |
| X509v3 CRL Distribution Points | X | False | | S | URI:URI of the CRL |
| subjectKeyIdentifier | X | False | | | |
| keyIdentifier | X | | | | This extension identifies the public key being certified. |
| X509v3 Basic Constraints | X | True | | | CA : FALSE |
| KeyUsage | X | True | | | |
| digitalSignature | X | | | S | True |
| certificatePolicies | X | False | | | |
| PolicyIdentifier | X | | | | Policy: 0.4.0.2042.1.2 Policy: 2.16.788.1.2.6.1.9 |
| OCSP No Check | X | | | S | |
| Extended Key Usage | X | False | | | |
| OCSP Signing | X | | | S | True |