PUBLIC

TrustFactory SSL Root CA Certification Practice Statement

Date:8th August 2018
Version: 1.3

Contents

Document History

Version	Description	Date
1.0	Initial for review	6 October 2017
1.1	Minor corrections Added certificate serial numbers and certificate profiles.	7 December 2017
1.2	Updates to Section 9.1 Fees Other minor corrections	15 December 2017
1.3	Minor edits (contact details) and updates for clarity	8 August 2018

Digitally Signed by: TrustFactory (Pty) Ltd

1.0 Introduction

This Certification Practice Statement (CPS) applies to the products and services of TrustFactory SSL Root Certification Authority (CA). The latest version may be found on the TrustFactory group company Repository at https://www.trustfactory.net/repository.

A CPS highlights the *"procedures under which a Certificate is issued to a particular community and/or class of application with common security requirements"*. This CPS aims to adhere to the content and structure guidance provided in Internet Engineering Task Force (IETF) RFC 3647, dated November 2003. Where certain sections or topics of the RFC do not apply or requirements not defined then the term 'No stipulation' is used.

TrustFactory CAs are governed by the TrustFactory Certificate Policy (CP) together with a Certification Practice Statement (CPS) applicable to the specific CA.

TrustFactory SSL Root CA 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 the Baseline Requirements, the Baseline Requirements take precedence over this document.

This CPS should be read together with the TrustFactory Certificate Policy. Certain practices, controls, compliance, business and legal matters that are common across all TrustFactory CAs are documented in the TrustFactory CP. This CPS addresses the specific technical and procedural practices of the TrustFactory SSL Root CA, within the TrustFactory PKI System, which issue Certificates to Issuing CAs.

1.1 Overview

This CPS applies to the following Certification Authorities managed by TrustFactory:

- **TrustFactory SSL Root CA**

The purpose of this CPS is to present the TrustFactory SSL Root CA practices and procedures in managing Root CA Certificates and to demonstrate compliance with requirements pertaining to the issuance of Certificates according to TrustFactory Certificate Policy (CP).

The Certificate names addressed in this CPS are the following:

- TrustFactory SSL Root Certificate Authority with serial number 01

1.2 Document Name and Identification

This document is the TrustFactory SSL Root CA Certification Practice Statement (TrustFactory SSL Root CA CPS).

The OID for TrustFactory is: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) trustfactory(50318)}

TrustFactory organizes its OID arcs for its CP and CPS documents as follows:

1.3.6.1.4.1.50318.1	TrustFactory CA CP
1.3.6.1.4.1. 50318.2.1	TrustFactory SSL Root CA Certificates Practice Statement
1.3.6.1.4.1. 50318.2.3	TrustFactory SSL Issuing CA Certificates Practice Statement

All TrustFactory CP and CPS documents are published in the Repository at https://www.trustfactory.net/repository.

1.3 PKI Participants

1.3.1 TrustFactory Root Certification Authorities

The TrustFactory Issuing CA's are chained into the trust hierarchy of the TrustFactory Root Certification Authority. This offers certificates with the following hierarchies:

- TrustFactory SSL Root Certification Authority
  - TrustFactory SSL Issuing Certification Authority
    - DomainPass Certificate
    - OrganizationPass Certificate

The TrustFactory SSL Root CA may:

• Accept the Certificate Signing Requests ("CSR") with the public keys of a TrustFactory SSL Issuing CA which has been approved by the TrustFactory Policy Authority and whose identity and verified information to be contained in the TrustFactory SSL Issuing CA Certificate have been established through a formal key ceremony;

• Create a TrustFactory SSL Issuing CA Certificate containing the signed public key, once the CSR is verified by the TrustFactory SSL Root CA.

1.3.2 Registration Authorities

The TrustFactory SSL Root CA will act as its own Registration Authority responsible for:

- Accepting, evaluating, approving or rejecting the registration of TrustFactory SSL Issuing CA Certificate applications;
- Issuance of a Certificate in accordance with the provisions of the TrustFactory SSL Root CA CPS; and
- Initiating the process to revoke a TrustFactory SSL Issuing CA certificate.

1.3.3 Subscribers

Subscribers are TrustFactory SSL Issuing CAs that have been issued a TrustFactory SSL Issuing CA Certificate.

1.3.4 Relying Parties

A Relying Party is a subordinate CA, person, entity, or organisation that relies on or uses the TrustFactory SSL Issuing CA Certificate and/or any other information provided in the TrustFactory repository to verify the identity and public key of a Subscriber.

Relying Parties must always refer to TrustFactory SSL Root CA's revocation information in the form of a CRL distribution point.

1.3.5 Other Participants

The CAs and RAs operating under the TrustFactory CP may require the services of other security, community, and application authorities.

1.4 Certificate Usage

1.4.1 Appropriate certificate usage

TrustFactory SSL Issuing CA Certificates may be used for the following purposes:

- Validating Certificates issued by the TrustFactory SSL Issuing CA's
- Validating Certificate Revocation Lists (CRL)) and OCSP Responses issued by the TrustFactory SSL Issuing CA's

Key Usage parameters are defined as:

- Certificate Signing
- Off-line CRL Signing
- CRL Signing

1.4.2 Prohibited Certificate usage

Certificate use is restricted by using Certificate extensions on key usage and extended key usage.

Any usage not defined in Section 1.4.1 above shall be deemed prohibited usage.

Any usage of the Certificate inconsistent with these extensions is not authorised. Certificates are not authorised for use for any transactions above the designated reliance limits that have been indicated in the TrustFactory Warranty Policy.

Certificates issued under this CPS may not be used:

- for any application requiring fail safe performance such as:
  - the operation of nuclear power facilities,
  - air traffic control systems,
  - aircraft navigation systems,
  - weapons control systems, and
  - any other system whose failure could lead to injury, death or environmental damage; or
- where prohibited by law.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Requests for information on the compliance of TrustFactory CAs with accreditation schemes as well as any other inquiry associated with this CP should be addressed to:

TrustFactory Policy Authority
c/o iSolv Technologies
TrustFactory General Manager
c/o iSolv Technologies
Firestation Rosebank, 6th Floor
16 Baker St, Rosebank,
Johannesburg, 2196
South Africa
Tel: +27-11-880 6103
Fax: +27-11-880 5443
Email: info@trustfactory.net

1.5.2 Contact Person

TrustFactory General Manager
c/o iSolv Technologies
Firestation Rosebank, 6th Floor
16 Baker St, Rosebank,
Johannesburg, 2196
South Africa
Tel: +27-11-880 6103
Fax: +27-11-880 5443
Email: info@trustfactory.net

1.5.3 Person Determining CPS Suitability for the Policy

The TrustFactory Policy Authority determines the suitability and applicability of this CPS and the conformance of this CPS to the TrustFactory CP based on the results and recommendations received from a Qualified Auditor. The Policy Authority shall approve this CPS.

1.5.4 CPS Approval Procedures

The TrustFactory Policy Authority reviews and approves any changes to this CPS. The updated CPS is reviewed against the CP in order to check for consistency. CP changes are also added on as needed basis. Upon approval of a CPS update by the Policy Authority, the new CPS is published in the TrustFactory SSL Root CA Repository at https://www.trustfactory.net/repository.

The updated version is binding upon all Subscribers, for all Certificates that have been issued or are to be issued, including the Subscribers and parties relying on Certificates that have been issued under a previous version of the CPS.

1.6 Definitions and acronyms

Any terms used but not defined herein shall have the meaning ascribed to them in the Baseline Requirements.

Adobe Approved Trust List (AATL): A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 9.0

Advanced Electronic Signature: A specific digital signature that complies to the requirements of the Electronic Communications & Transactions Act in South Africa, and can be relied on for evidence in a court of law.

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 Legal Entity is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.

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 Identity Information is correct.

Business Entity: Any entity that is not a Private Organization, Government Entity, or non-commercial entity as defined in the EV Guidelines. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

CDS (Certified Document Services): A document signing architecture created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 6.0.

Certificate: An electronic document that uses a Digital Signature to bind a Public Key and an identity.

Certificate Beneficiaries: The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate, all Application Software Suppliers with whom TrustFactory Issuing CA 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.

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

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

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

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

Certificate Request: Communications described in Section 10 of the Baseline Requirements requesting the issuance of a Certificate.

Certificate Revocation List: A regularly updated timestamped 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.

Compromise: A violation of a security policy that results in loss of control over sensitive information.

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

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

Digital Signature: To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Name System: An Internet service that translates Domain Names into IP addresses.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

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

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

ECT Act: The Electronic Communications and Transactions Act of the Government of South Africa.

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization or its subsidiaries. An Enterprise RA may also authorize issuance of client authentication Certificates to partners, customers, or affiliates wishing to interact with that organization.

Expiry Date: The "notAfter" date in a Certificate that defines the end of a Certificate's Validity Period.

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

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

Hash (e.g. SHA1 or SHA256): An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

Hardware Security Module (HSM): An HSM is type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.

Incorporate by Reference: To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

Incorporating Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Individual: A natural person.

Internationalized Domain Name (IDN): An internet domain name containing at least one language-specific script or alphabetic character which is then encoded in punycode for use in DNS which accepts only ASCII strings.

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.

Jurisdiction of Incorporation: In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Key Compromise: A Private Key is said to be Compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

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

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with

legal standing in a Country's legal system.

Object Identifier (OID): 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.

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc.) where the Applicant's business is conducted.

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.

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.

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 (PKI): 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 (Identity/ Qualifications of Assessor).

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

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

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.

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. For TrustFactory the Repository is at https://www.trustfactory.net/repository

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.

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 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 or Terms of Use.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

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

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance

with the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA.

Trusted Platform Module (TPM): A hardware cryptographic device which is defined by the Trusted Computing Group. https://www.trustedcomputinggroup.org/specs/TPM.

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.

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

Vetting Agent: Someone who performs the information verification duties specified by the Baseline Requirements.

WebTrust Program for CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

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.

X.509: The standard of the ITU-T (International Telecommunications Union-T) for Certificates.

AATL	Adobe Approved Trust List
AES	Advanced Electronic Signature
AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
EKU	Extended Key Usage
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
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
ID	Identity document
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PKI	Public Key Infrastructure
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority
RFC	Request for Comments
SAAA	South African Accreditation Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VAT	Value Added Tax

2.0 Publication and Repository Responsibilities

2.1 Repositories

TrustFactory SSL Root CA publishes all CA Certificates, revocation data for issued Certificates, CP, CPS, and Relying Party agreements and Subscriber Agreements in Repositories. The legal repository for all TrustFactory CA public facing documentation is https://www.trustfactory.net/repository

TrustFactory SSL Root CA refrains from making publicly available sensitive and/or confidential documentation including security controls, operating procedures and internal security policies. These documents are, however, made available to Qualified Auditors as required during any WebTrust or SAAA audit performed on TrustFactory SSL Root CA.

2.2 Publication of Certificate Information

TrustFactory SSL Root CA publishes its CP, CPS, Subscriber Agreements, and Relying Party agreements at https://www.trustfactory.net/repository.

CRLs are published in online repositories. The CRLs contain entries for all revoked unexpired Certificates with a validity period that depends on Certificate type and/or position of the Certificate within the Certificate chain.

The TrustFactory SSL Root CA Certificate Revocation List is accessible through the web-interface at: http://www.trustfactory.net/crl/tf-rca.crl

The Root CA shall ensure that revocation data for issued Certificates and its Root Certificate are available through a Repository 24 hours a day, 7 days a week.

2.3 Time or Frequency of Publication

The TrustFactory PA shall annually review this CPS and may make revisions and updates to policies as required by changes in standards, laws and regulations or other circumstances. Any updates become binding for all Certificates that have been issued or are to be issued upon the date of the publication of the updated version of this CPS.

New or modified versions of the CP, this CPS, Subscriber Agreements, or Relying Party agreements are published within ten days after being digitally signed by the TrustFactory Policy Authority.

2.4 Access control on repositories

The repository is publicly accessible information with Read-only access for the public.

Access control policies are implemented to prevent unauthorized persons from adding, deleting, or modifying repository entries. TrustFactory ensures that the integrity and authenticity of its public documentation is maintained by digitally signing the Adobe PDF format of the documents.

3.0 Identification and Authentication

TrustFactory SSL Root CA acts as its own RA for issuance of an Issuing CA Certificate .

3.1 Naming

3.1.1 Types of Names

TrustFactory SSL Root CA Certificates are issued with subject DNs (Distinguished Names) which meet the requirements of X.500 naming. Common Names (CNs) respect name space uniqueness and are not misleading.

The common name shall be the name associated with the SSL Issuing CA Certificate to be issued.

3.1.2 Need for Names to be Meaningful

The value of the common name attribute used is the name associated with the specific TrustFactory Issuing CA and should represent its specific purpose (e.g. SSL or Client).

3.1.3 Anonymity or Pseudonymity of Subscribers

Pseudonyms (names other than a subscriber's true organisational name) shall not be permitted, except for the purposes of issuing certificates for testing or demonstration purposes.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

In the provision of Issuing CA certificates the CA names and other attributes in the certificate distinguished name of the Issuing CA will provide a unique name.

3.1.5 Uniqueness of Names

TrustFactory SSL Root CA enforces the uniqueness of each Subject name in a Certificate Authority as follows:

- The combination of the Common Name and all the attributes of the Distinguished Name (DN), together with the certificate serial number provides a unique electronic identity for the Issuing CA.

3.1.6 Recognition, Authentication, and Role of Trademarks

TrustFactory SSL Root CA may not use registered trademarks when assigning the distinguished names to Issuing CA's.

3.2 Initial Identity Validation

Not applicable since the same entity owns the TrustFactory SSL Root CA and subsequent SSL Issuing CAs. However the TrustFactory PA will validate that requests for Issuing CA Certificates are only submitted by the authorized TrustFactory management personnel.

3.2.1 Method to Prove Possession of Private Key

The Issuing CA should generate a Certificate Signing Request (CSR) signed with its Private Key and the TrustFactory SSL Root CA will validate it with the Issuing CA's public key.

This requirement does not apply where a key pair is generated by the Root CA on behalf of the Issuing CA.

3.2.2 Authentication of Organization Identity & Doman Identity

The TrustFactory PA shall verify and validate all the information required in the TrustFactory SSL Issuing CA certificate.

3.2.3 Authentication of Individual identity

Not applicable since the TrustFactory SSL Root CA will not accept requests for individual certificates.

3.2.4 Non Verified Subscriber Information

Information that is not verified shall not be included in certificates

3.2.5 Validation of Authority

The PA will validate that requests related to SSL Issuing CA Certificates, such as initial registration, renewal or revocation, are only submitted by the authorized TrustFactory management personnel.

3.2.6 Criteria for Interoperation

Not applicable

3.3 Identification and Authentication for Renewal Requests

TrustFactory PA will validate that requests for renewal of Issuing CA Certificates are only submitted by the authorized TrustFactory management personnel.

The TrustFactory PA shall verify and validate all the information required in the renewed TrustFactory SSL Issuing CA certificate.

The certificate renewal is authenticated when the SSL Issuing CA submits a Certificate Signing Request (CSR) signed with its Private Key and the TrustFactory SSL Root CA will validate it with the SSL Issuing CA's public key.

3.4 Identification and Authentication for Re-key Requests

TrustFactory SSL Root CA does not support re-key requests for SSL Issuing CAs.
The SSL Issuing CA is required to go through the initial registration process described in Section 4.1 in this document to obtain a new Certificate.

3.4.1 Identification and Authentication for Routine Re-key

No stipulation

3.4.2 Identification and Authentication for Reissuance after Revocation

Reissue after revocation is not supported.
The SSL Issuing CA is required to go through the initial registration process described in Section 4.1 in this document to obtain a new Certificate.

3.4.3 Re-verification and Revalidation of Identity When Certificate Information Changes

If at any point any Subject name information embodied in a Certificate is to be changed in any way, the TrustFactory PA must validate and approve the change and a new Certificate issued with the validated information.

3.4.4 Identification and Authentication for Re-key After Revocation

A routine re-key after revocation is not supported.
The SSL Issuing CA is required to go through the initial registration process described in Section 4.1 in this document to obtain a new Certificate.

3.5 Identification and Authentication for Revocation Request

All revocation requests are authenticated by TrustFactory SSL Root CA operations team. Revocation of an Issuing CA has to be approved by the TrustFactory General Manager or PA.

4.0 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

TrustFactory GM will submit the request to the PA for creation of a new Issuing CA.

4.1.2 Enrollment Process and Responsibilities

The application process requires the following steps:

1. TrustFactory General Manager will complete an application for an SSL Issuing CA and submit to the TrustFactory PA.
2. The TrustFactory PA shall verify and validate all the information required in the SSL Issuing CA certificate.
3. TrustFactory PA may approve or reject the request for an SSL Issuing CA certificate.

The enrolment process includes the following steps:

- TrustFactory operations schedules a key ceremony at the TrustFactory SSL Root CA vault to establish the Issuing CA
- Conduct key generation for the new Issuing CA in the Issuing CA HSM
- During the key ceremony, submit a CSR from the SSL Issuing CA to the TrustFactory SSL Root CA;
- The TrustFactory SSL Root CA will validate and sign the SSL Issuing CA CSR and issue the Issuing CA Certificate;
- install the SSL Issuing CA Certificate on the Issuing CA system.
- Clone new keys and certificate to backup HSM

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The TrustFactory PA will validate that requests for Issuing CA Certificates are only submitted by the authorized TrustFactory management personnel.

Refer to 3.2 above

4.2.2 Approval or Rejection of Certificate Applications

TrustFactory PA may approve the request for an SSL Issuing CA certificate, assuming all verification of certificate information can be completed successfully. The TrustFactory PA may reject applications including for the following reasons:

- TrustFactory PA is unable to successfully verify or validate the information to be published on the SSL Issuing CA Certificate
- TrustFactory PA may reject requests based on potential brand damage to TrustFactory SSL Root CA in accepting the request.

TrustFactory PA is under no obligation to provide a reason for rejection of a Certificate Request..

4.2.3 Time to Process Certificate Applications

All reasonable methods are used in order to evaluate and process Certificate applications within one month from receipt of completed application.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

TrustFactory SSL Root CA can only accept certificate issuance requests for SSL Issuing CAs approved by the TrustFactory PA. The PA must satisfy itself that the information provided to it by the SSL Issuing CA is accurate and that the verification checks have been successfully completed.

After approval by the PA, the TrustFactory GM shall arrange for the creation and operation of the new Issuing CA and submit a CSR from the SSL Issuing CA to the TrustFactory SSL Root CA. The TrustFactory SSL Root CA may then generate and digitally sign the Issuing CA Certificate applied for.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

TrustFactory General Manager will provide written confirmation to the PA of issuance of the Issuing CA certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

After issuance of the SSL Issuing CA certificate, the TrustFactory operations team will check that the certificate content is accurate. If there are any inaccuracies then the certificate will be revoked.

The Certificate is deemed accepted when the SSL Issuing CA starts using the Certificate.

4.4.2 Publication of the Certificate by the CA

TrustFactory SSL Root CA publishes the Certificate by publishing it in a Repository at https://www.trustfactory.net/repository

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The TrustFactory Policy Authority must be notified whenever an Issuing CA certificate is issued. Notification to other entities is not required.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The TrustFactory SSL Issuing CA shall use its private key and Certificate in strict compliance with this CPS. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding Certificate.

Refer to certificate profiles in Annexure A.

4.5.2 Relying Party Public Key and Certificate Usage

TrustFactory provides a Relying Party Agreement that Relying Parties should comply with. Relying Parties should check the status of the SSL Issuing CA certificate before relying on the certificate and perform a risk assessment to ensure that their reliance is appropriate according to the defined key usage.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

TrustFactory SSL Root CA may renew a Certificate so long as:-

- The original Certificate to be renewed has not been revoked;
- The original Certificate to be renewed has not expired;
- The Public Key from the original Certificate has not been blacklisted for any reason; and
- All details within the Certificate remain accurate and no new or additional validation is required.

The original Certificate must be revoked after renewal is complete.

4.6.2 Who May Request Renewal

The TrustFactory General Manager should submit a request to the PA for approval of the renewal of the Issuing CA certificate.

4.6.3 Processing Certificate Renewal Requests

A CSR must be used with the same Public Key to be certified as in the original certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewed Certificate

As per 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.7 Certificate Re-Key

TrustFactory SSL Root CA does not support certificate re-key for Issuing CA Certificates.

4.8 Certificate Modification

Modifying a certificate is not permitted. The process for revocation and new certificate application should be followed if a modification is required.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Revocation of an SSL Issuing CA Certificate shall be performed within twenty-four (24) hours under one or more of the following circumstances as identified by the TrustFactory management team:

1. The TrustFactory General Manager requests revocation in writing;
2. The TrustFactory General Manager notifies the Policy Authority that the original certificate request was not authorized and does not retroactively grant authorization;
3. The TrustFactory operations obtains evidence that the SSL Issuing 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. The TrustFactory CA operations obtains evidence that the Certificate was misused;
5. The TrustFactory CA operations is made aware that the Certificate was not issued in accordance with or that Issuing CA has not complied with this CP or the applicable Certificate Policy or Certification Practice Statement;
6. The TrustFactory CA operations determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The TrustFactory SSL Root CA or TrustFactory SSL Issuing CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The TrustFactory SSL Root CA's or TrustFactory SSL Issuing CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the SSL Root CA has made arrangements to continue maintaining the CRL Repository;
9. Revocation is required by the TrustFactory SSL Root CA's Certificate Policy and/or Certification Practice Statement; or
10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time)

4.9.2 Who Can Request Revocation

The TrustFactory management or operations team may request revocation of a TrustFactory SSL Issuing CA Certificate if there is reasonable cause to revoke the certificate.

Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the Issuing CA of reasonable cause to revoke the certificate

4.9.3 Procedure for Revocation Request

TrustFactory operations will record each request for revocation and authenticate the source, taking appropriate action to revoke the Certificate if the request is authentic and approved.

The TrustFactory operations team will generate a CRL signing request for an updated CRL containing the serial number of the CA Certificate that needs to be revoked, and manually sign the CRL using the offline SSL Root CA.

Once revoked, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason codes may be included. CRLs are published according to this CPS.

TrustFactory provides Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The instructions are provided through the TrustFactory website at www.trustfactory.net

TrustFactory SSL Root CA does not support bulk revocation.

4.9.4 Revocation Request Grace Period

Revocation requests shall be actioned as soon as reasonably practicable following verification of the revocation request.

4.9.5 Time Within Which CA Must Process the Revocation Request

TrustFactory operations shall begin investigating Certificate Problem Reports within twenty-four (24) hours of receipt of the report. and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
4. Relevant legislation.

TrustFactory SSL Root CA will revoke Issuing CA certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests received within four hours of CRL issuance.

4.9.6 Revocation Checking Requirements for Relying Parties

Prior to relying upon a Certificate, Relying Parties must validate the suitability of the Certificate to the purpose intended and ensure the Certificate is valid. Relying Parties will need to consult the CRL information for each Certificate in the chain as well as validating that the Certificate chain itself is complete and follows IETF PKIX standards.

4.9.7 CRL Issuance Frequency

For the status of Issuing CA Certificates:

The TrustFactory Root CA shall update and reissue CRLs at least:

(i) once every twelve months; and

(ii) within 24 hours after revoking an SSL Issuing CA Certificate; and

the value of the nextUpdate field will not be more than twelve months beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

No stipulation

4.9.9 On-Line Revocation Status Checking Availability

CRLs are published in online repositories.

The TrustFactory SSL Root CA Certificate Revocation List is accessible through the web-interface at: http://www.trustfactory.net/crl/tf-rca.crl

The Root CA shall ensure that revocation data for issued Certificates and its Root Certificate are available through a Repository 24 hours a day, 7 days a week.

4.9.10 On-Line Revocation Checking Requirements

The TrustFactory SSL Root CA updates information provided via an Online Certificate Status Protocol at least (i) once every twelve months and (ii) within 24 hours after revoking an Issuing/Subordinate CA Certificate.

Relying Parties must confirm revocation information otherwise all warranties becomes void.
The SSL Root CA does not sign error messages when returned in response to certificate status requests.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements Related to Key Compromise

In the event of compromise of a TrustFactory SSL Root CA Private Key used to sign SSL Issuing CA Certificates, TrustFactory operations will as soon as practically possible inform the SSL Issuing CA that the private key may have been Compromised. This includes cases where TrustFactory operations at its own discretion decides that evidence suggests a possible Key Compromise has taken place.

Where Key Compromise is not disputed, TrustFactory SSL Root CA shall revoke Issuing CA Certificates within 24 hours and publish online CRLs within 4 hours of creation.

4.9.13 Notification of Certificate Revocation to Subscriber

The TrustFactory General Manager shall notify the TrustFactory PA of the revocation of an Issuing CA Certificate, and a notice is placed on the Repository.

4.9.14 Circumstances for Suspension

Certificate suspension is not supported and not permitted

4.10 Certificate Status Services

4.10.1 Operational Characteristics

TrustFactory SSL Root CA provides a Certificate status service in the form of a CRL distribution point. These services are presented to Relying Parties within the Certificate and the URLs to access the CRL are provided in Section 2.2 of this CPS.

Revocation entries on a CRL are not be removed until after the Expiry Date of the revoked Certificate CRLs are signed by the TrustFactory SSL Root CA Private Key.

4.10.2 Service Availability

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

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

4.10.3 Operational Features

No stipulation

4.10.4 End of Subscription

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

4.11 Key Escrow and Recovery

4.11.1 Key Escrow and Recovery Policy and Practices

CA Private Keys are never escrowed. TrustFactory SSL Root CA does not offer key escrow services.

4.11.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5.0 Facility, Management, and Operational Controls

TrustFactory SSL Root CA operate under physical and environmental security policies designed to provide reasonable assurance of the detection, deterrence and prevention of unauthorized logical or physical access to CA related facilities..

5.1 Physical Controls

Controls are as defined in the TrustFactory CP

5.2 Procedural Controls

Controls are as defined in the TrustFactory CP

5.3 Personnel Controls

Controls are as defined in the TrustFactory CP

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files shall be generated for events relating to the security and services of the CA. Where possible, the security audit logs shall be automatically generated. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

TrustFactory SSL Root CA records at least the following events:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction;
        - Withdrawal of keying material from service;
        - Identity of the entity authorizing a key management operation,
        - Identity of entity handling any keying material (such as key components or keys stored in portable devices or media);
        - Compromise of a private key;
    b. Cryptographic device lifecycle management events:
        - device receipt and installation;
        - placing into or removing a device from storage;
        - device activation and usage;
        - device changes in state of use
2. CA and Subscriber Certificate lifecycle management events, including:
    a. Certificate requests, renewal, and revocation;
    b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
    c. Acceptance and rejection of CA certificate requests by the TrustFactory PA;
    d. Issuance of Certificates;
    e. Generation of Certificate Revocation Lists.
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes;
    d. System crashes, hardware failures, and other anomalies;
    e. Firewall and router activities; and
    f. Entries to and exits from the CA facility.

At a minimum, each audit record includes the following (either recorded automatically or manually) elements:

- Date and time of the entry;
- Identity of the person or entity making the journal entry; and
- Description of the entry.

5.4.2 Frequency of Processing Log

Audit logs are reviewed on a weekly basis by the TrustFactory Security Officer for any evidence of malicious activity and following each important operation. Unauthorized or suspicious activity is investigated.

5.4.3 Retention Period for Audit Log

Audit log records are retained for at least seven years or held for a period of time as appropriate to provide necessary legal evidence in accordance with any applicable legislation. Records may be required at least as

long as any transaction relying on a Valid Certificate can be questioned.

5.4.4 Protection of Audit Log

The events are logged in a way that they cannot be deleted or destroyed (except for transfer to long term media) for any period of time that they are retained.

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

Digital signatures are used to protect the integrity of audit logs where applicable or required to satisfy legal requirements.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries are backed-up using online backup mechanism to the disaster recovery site. However they remain under the control of an authorized trusted role, and separated from their component source generation. Audit log backup is protected to the same degree as originals.

5.4.6 Audit Collection System (Internal vs. External)

Audit processes are initiated at system start up and finish only at system shutdown. The audit collection system ensures the integrity and availability of the data collected. In the case of a problem occurring during the process of the audit collection TrustFactory determines whether to suspend TrustFactory SSL Root CA operations until the problem is resolved, duly informing the TrustFactory impacted users.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

TrustFactory SSL Root CA performs regular vulnerability assessments covering all Root CA systems related to Certificate issuance, products and services.
Additionally, the CA's security program includes 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 the CA has in place to counter such threats

5.5 Records Archival

5.5.1 Types of Records Archived

TrustFactory CAs archive records with enough detail to establish the validity of a signature and of the proper operation of the CA system. The records that are archived are listed in section 5.4.1.

5.5.2 Retention Period for Archive

The minimum retention period for archive audit log data is seven years after Certificate expiry.

5.5.3 Protection of Archive

The archives are created in such a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time for which they are required to be held. Archive protections ensure that only authorized trusted access is able to make operations without modifying integrity, authenticity and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

5.5.4 Archive Backup Procedures

Archive data is backed up over the network to a storage media within the DR data center vault.

Paper records are transferred to a secure storage facility that is access controlled.

5.5.5 Requirements for Timestamping of Records

TrustFactory Root CAs do not use a time stamp service. All logs have data indicating the time at which the event occurred..

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing of TrustFactory SSL Root CA archive information is checked upon creation.
Only authorised TrustFactory SSL Root CA equipment, trusted role and other authorized persons are allowed to access the archive. Requests to obtain archive information are coordinated by operators in trusted roles (auditor, the manager in charge of the process and the security officer).

5.6 Key Changeover

Towards the end of each private key's lifetime, in accordance with Section 6.3.2, a new CA signing key pair is commissioned by TrustFactory and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both keys may be concurrently active. Private Keys used to sign previous SSL Issuing CA Certificates are maintained until such time as all SSL Issuing CA Certificates have expired. Certificate Subject information may also be changed and Certificate profiles may be altered to adhere to best practices.

The corresponding new CA Certificate is provided to Subscribers and relying parties through the online repository at www.trustfactory.net/repository.

5.7 Compromise and Disaster Recovery

Controls are as defined in the TrustFactory CP

5.8 CA or RA Termination

Controls are as defined in the TrustFactory CP

6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The signing key pair for the TrustFactory SSL Root CA was created during the initial start up of the CA application and is protected by the master keys for the TrustFactory SSL Root CA. Hardware key generation is used which is compliant to FIPS 140-2 level 3 and uses FIPS 186-2 key generation techniques.

TrustFactory SSL Root CA generates its CA Key Pairs under the following conditions:
1. in a physically secured environment, that has access control;
2. using personnel in trusted roles under the principles of multiple person control and split knowledge,
3. generate the CA keys within a cryptographic module which is certified at least to FIPS 140-2 level 3 or above;
4. log its CA key generation activities;
5. prepares and follows a Key Generation Script; and
6. witnessed by a qualified independent auditor.

6.1.2 Private Key Delivery to Subscriber

No stipulation

6.1.3 Public Key Delivery to Certificate Issuer

TrustFactory SSL Root CA only accepts Public Keys from TrustFactory Issuing CAs that are delivered to the TrustFactory SSL Root CA through a PKCS#10 Certificate Signing Request (CSR) as part of the Certificate Issuance process included in a formal key generation ceremony.

6.1.4 CA Public Key Delivery to Relying Parties

The TrustFactory SSL Root CA ensures that its Public Keys are delivered to Relying Parties in such a way as to prevent substitution attacks.

TrustFactory SSL Root CA Public Keys are available via a TrustFactory Repository at https://www.trustfactory.net/repository

6.1.5 Key Sizes

The TrustFactory SSL Root CA utilizes a key size of 4096 bits (RSA) with Hash Algorithm SHA-256. All new Subordinate CA's shall have a minimum key size of 2048-bit RSA.

Certificates meet the following requirements for algorithm type and key size.

Root CA Certificates

Digest algorithm	SHA- 256, SHA-384 or SHA- 512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits) ***	L= 2048, N= 224 or L= 2048, N= 256,

Subordinate CA Certificates

Digest algorithm	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)***	L= 2048, N= 224 Or L= 2048, N= 256

*** L and N (the bit lengths of modulus p and divisor q, respectively) are described in the Digital

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs

6.1.6 Public Key Parameters Generation and Quality Checking

TrustFactory SSL Root CA generates Key Pairs in accordance with FIPS 186.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

TrustFactory SSL Root CA sets key usage and enhanced usage of subordinate TrustFactory Issuing CA Certificates via the Key Usage Field for X.509 v3 (see Section 7.1).

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

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
4. Certificates for CRL/OCSP verification.

Key Usage for the TrustFactory SSL Root CA Certificate is set as:

- Certificate Signing
- Off-line CRL Signing
- CRL Signing

Key Usage for the TrustFactory SSL Issuing CA Certificate is set as:

- Certificate Signing
- Off-line CRL Signing
- CRL Signing

Enhanced Key Usage for the TrustFactory SSL Issuing CA Certificate is set as:

- Server Authentication
- Client Authentication
- Secure Email
- Time Stamping
- OCSP Signing

Any other use not specified above is prohibited.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Controls as per the TrustFactory CP

6.2.2 Private Key (n out of m) Multi-Person Control

Controls as per the TrustFactory CP

6.2.3 Private Key Escrow

Controls as per the TrustFactory CP

6.2.4 Private Key Backup

Controls as per the TrustFactory CP

6.2.5 Private Key Archival

Controls as per the TrustFactory CP

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Controls as per the TrustFactory CP

6.2.7 Private Key Storage on Cryptographic Module

Controls as per the TrustFactory CP

6.2.8 Method of Activating Private Key

Controls as per the TrustFactory CP

6.2.9 Method of Deactivating Private Key

Controls as per the TrustFactory CP

6.2.10 Method of Destroying Private Key

Controls as per the TrustFactory CP

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

TrustFactory SSL Root CA archives Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

TrustFactory SSL Root CA Certificates and renewed Certificates have a maximum Validity Period of 30 years.

TrustFactory SSL Issuing CA Certificates and renewed Certificates have a maximum Validity Period of 15 years.

TrustFactory SSL Root CA complies with the Baseline Requirements with respect to the maximum Validity Period.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of TrustFactory SSL Root CA activation data used to activate TrustFactory SSL Root CA Private Keys are made during a key ceremony (Refer to Section 6.1.1). Activation data is generated automatically by the appropriate HSM. It is then delivered to a holder of a share of the key who is a person in a trusted role. The delivery method maintains the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

TrustFactory SSL Root CA activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms. TrustFactory SSL Root CA activation data is stored on hardware tokens.

6.4.3 Other Aspects of Activation Data

TrustFactory SSL Root CA activation data may only be held by personnel in trusted roles.

6.5 Computer Security Controls

Controls as per the TrustFactory CP

6.6 Lifecycle Technical Controls

Controls as per the TrustFactory CP

6.7 Network Security Controls

Controls as per the TrustFactory CP

6.8 Time Stamping

Controls as per the TrustFactory CP

7.0 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Typical content of information published on a TrustFactory SSL Issuing CA Certificate includes but is not limited to the following elements of information:

- Serial number
- Signature algorithm
- Signature hash algorithm
- Issuer
- Valid from
- Valid to
- Subject
- Public key
- Basic Constraints
- Key Usage
- Authority Information Access
- Certificate Policies
- CRL Distribution Points
- Enhanced key usage

Certificate profiles are provided in Annexure A.

7.1.1 Version Number(s)

TrustFactory SSL Root CA issues Certificates in compliance with X.509 Version 3.

7.1.2 Certificate Extensions

TrustFactory SSL Root CA issues Certificates in compliance with RFC 5280 and meets the requirements for Certificate content and extensions as specified in the Baseline Requirements.

Root CA Certificate

a. basicConstraints
This extension is set as a critical extension. The cA field is set true.
b. keyUsage
This extension is set as a critical extension.
Bit positions for keyCertSign and cRLSign are set.
c. certificatePolicies
This extension is not present.
d. extendedKeyUsage
This extension is not present.

Issuing CA Certificate

a. certificatePolicies
This extension is not set as critical.
certificatePolicies:policyIdentifier is populated in accordance to Section 1.2
b. cRLDistributionPoints
This extension is not set as critical. and it contains the HTTP URL of the CA's CRL service.
c. authorityInformationAccess
This extension is not set as critical. and it contains the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).
d. basicConstraints
This extension is set as a critical extension. The cA field is set true
e. keyUsage
This extension is set as a critical extension.
This extension MUST be present and MUST be marked critical.
Bit positions for digitalSignature , keyCertSign and cRLSign are set.
f. extkeyUsage (optional)
This extension is not set as critical. The parameters are populated in accordance with Section 6.1.7 (and comply with RFC 5280).

All Certificates

All other fields and extensions are set in accordance with RFC 5280. The CA SHALL NOT issue a Certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in section 7.1.2.

7.1.3 Algorithm Object Identifiers

No stipulation.

7.1.4 Name Forms

TrustFactory SSL Root CA issues Certificates with name forms compliant to RFC 5280.
By issuing an SSL Issuing CA Certificate, the TrustFactory SSL Root CA represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

The following **Subject Distinguished Name Fields** are populated in accordance with profile in Annexure A:

a. **Certificate Field:** subject:commonName
b. **Certificate Field:** subject:organizationName
c. **Certificate Field:** subject:countryName

7.1.5 Name Constraints

TrustFactory SSL Root CA may issue Certificates with name constraints where necessary and mark as critical where necessary.

7.1.6 Certificate Policy Object Identifier

The TrustFactory SSL Root CA Certificate does not contain the certificatePolicies extension.

TrustFactory SSL Root CA issues certificates that comply with the latest version of the CAB Forum Baseline Requirements.

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

7.2.1 Version Number(s)

TrustFactory SSL Root CA issues Version 2 CRLs in compliance with RFC 5280. CRLs have the following fields:

- **Issuer:**
  CN = TrustFactory SSL Root Certificate Authority
  OU = TrustFactory PKI Operations
  O = TrustFactory(Pty)Ltd
  L = Johannesburg
  S = Gauteng
  C = ZA
- **Effective date** Date and Time issued
- **Next update** Date and Time of next issue
- **Signature Algorithm** sha256RSA
- **Signature Hash Algorithm** sha256
- **Serial Number(s)** List of revoked serial numbers
- **Revocation Date** Date of Revocation

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:

- **CRL Number** Monotonically increasing serial number for each CRL
- **Authority Key Identifier** AKI of the issuing CA for chaining/validation requirements

7.3 OCSP Profile

TrustFactory SSL Root CA does not operate an Online Certificate Status Profile (OCSP) responder.

8 Compliance Audit and Other Assessments

The procedures within this CPS encompass all relevant portions of currently applicable PKI standards for the various vertical PKI industries in which TrustFactory SSL Root CA operates. CAs are audited for compliance to one or more of the following standards:-

- AICPA/CICA Trust Service Principles and Criteria for Certification Authorities
- AICPA/CICA WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

8.1 Frequency and Circumstances of Assessment

Controls as per the TrustFactory CP

8.2 Identity/Qualifications of Assessor

Controls as per the TrustFactory CP

8.3 Assessor's Relationship to Assessed Entity

Controls as per the TrustFactory CP

8.4 Topics Covered by Assessment

Controls as per the TrustFactory CP

8.5 Actions Taken as a Result of Deficiency

Controls as per the TrustFactory CP

8.6 Communications of Results

Controls as per the TrustFactory CP

9.0 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Controls as per the TrustFactory CP

9.1.2 Certificate Access Fees

Controls as per the TrustFactory CP

9.1.3 Revocation or Status Information Access Fees

Controls as per the TrustFactory CP

9.1.4 Fees for Other Services

Controls as per the TrustFactory CP

9.1.5 Refund Policy

Controls as per the TrustFactory CP

9.2 Financial Responsibility

Controls as per the TrustFactory CP

9.3 Confidentiality of Business Information

Controls as per the TrustFactory CP

9.4 Privacy of Personal Information

Controls as per the TrustFactory CP

9.5 Intellectual Property rights

Controls as per the TrustFactory CP

9.6 Representations and Warranties

Controls as per the TrustFactory CP

9.7 Disclaimers of Warranties

Controls as per the TrustFactory CP

9.8 Limitations of Liability

Controls as per the TrustFactory CP

9.9 Indemnities

Controls as per the TrustFactory CP

9.10 Term and Termination

Controls as per the TrustFactory CP

9.11 Individual Notices and Communications with Participants

Controls as per the TrustFactory CP

9.12 Amendments

Controls as per the TrustFactory CP

9.13 Dispute Resolution Provisions

Controls as per the TrustFactory CP

9.14 Governing Law

Controls as per the TrustFactory CP

9.15 Compliance with Applicable Law

Controls as per the TrustFactory CP

9.16 Miscellaneous Provisions

Controls as per the TrustFactory CP

10 Annexure: SSL CA Certificate Profiles

10.1 TrustFactory SSL Root CA – Certificate Profile

V1 Fields	
Version	V3
Serial number	01
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CN = TrustFactory SSL Root Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA
Valid from	Tuesday, December 5, 2017 12:59:29 PM
Valid to	Thursday, November 28, 2047 12:59:29 PM
Subject	CN = TrustFactory SSL Root Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA
Public key	RSA (4096 bits)
Critical Extensions	
Basic Constraints	Subject Type=CA
	Path Length Constraint=None
Key Usage	Certificate Signing Off-line CRL Signing CRL Signing
Extensions	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.trustfactory.net/crl/tf-rca.crl CRL Reason=Key Compromise, CA Compromise (60)
Properties	
Thumbprint algorithm	SHA1

10.2 TrustFactory SSL Issuing CA – Certificate Profile

V1 Fields	
Version	V3
Serial number	03
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CN=TrustFactory SSL Root Certificate Authority O=TrustFactory(Pty)Ltd C=ZA
Valid from	Tuesday, December 5, 2017 2:23:47 PM
Valid to	Wednesday, December 1, 2032 2:23:47 PM
Subject	CN = TrustFactory SSL Issuing Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA
Public key	RSA (4096 bits)
Critical Extensions	
Basic Constraints	Subject Type=CA
	Path Length Constraint=None
Key Usage	Certificate Signing Off-line CRL Signing CRL Signing
Extensions	
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.trustfactory.net/tf-ssl-issuing
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.50318.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.trustfactory.net/repository
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.trustfactory.net/crl/tf-ssl-issuing.crl
Properties	
Thumbprint algorithm	SHA1
Enhanced key usage (property)	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Time Stamping (1.3.6.1.5.5.7.3.8) OCSP Signing (1.3.6.1.5.5.7.3.9)