PUBLIC

TrustFactory SSL Issuing CA Certification Practice Statement

Date: 15 December 2017
Version: 1.2

Contents

Document History

Version	Description	Date
1.0	Initial for review	6 October 2017
1.1	Error 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

1.0 Introduction

This Certification Practice Statement (CPS) applies to the products and services of TrustFactory SSL Issuing CA. Primarily this pertains to the issuance and lifecycle management of Certificates including validity checking services. The latest version may be found on the TrustFactory 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 SSL Issuing 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.

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

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 Issuing CA, within the TrustFactory PKI System, that issue Certificates to web servers.

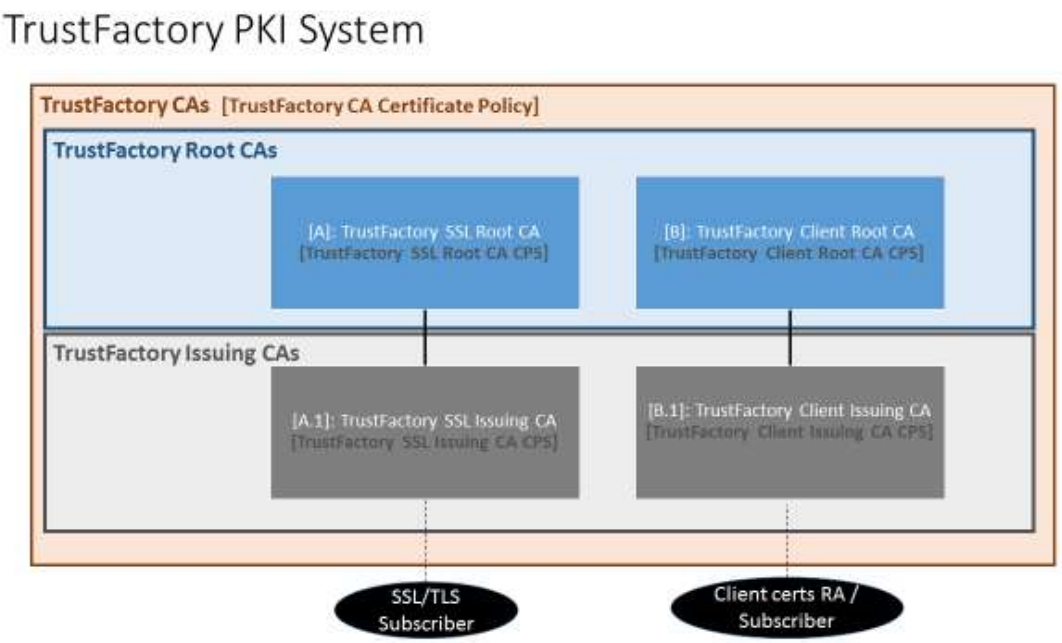

Figure 1: TrustFactory PKI System

1.1 Overview

The TrustFactory CP and this CPS applies to the of the following Certification Authorities, that issue public certificates, managed by TrustFactory:

A.1: **TrustFactory SSL Issuing CA**

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

The Certificate names addressed in this CPS are the following:

- TrustFactory SSL Issuing Certificate Authority – with serial number 03

1.2 Document Name and Identification

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

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

TrustFactory organizes the 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

1.3 PKI Participants

1.3.1 TrustFactory Certification Authorities

The TrustFactory SSL Issuing CA is chained into the trust hierarchy of the TrustFactory Root Certification Authority. This offers certificates with the following hierarchy:

- [A] TrustFactory SSL Root Certification Authority
  - [A.1] TrustFactory SSL Issuing Certification Authority
    - SSL/TLS Domain Validation Subscriber
    - SSL/TLS Organization Validation Subscriber

- [B] TrustFactory Client Root Certification Authority
  - [B.1] TrustFactory Client Issuing Certification Authority
    - Personal Certificate Subscriber / RA
    - Advanced Electronic Signature Certificate Subscriber / RA
    - Email Certificate Subscriber / RA

The TrustFactory SSL Issuing CA is a Certification Authority that issues Certificates in accordance with this CPS. As a Certification Authority, TrustFactory SSL Issuing CA is responsible for managing the certificate lifecycle management tasks related to: Subscriber registration, Certificate issuance, renewal, distribution and revocation. TrustFactory SSL Issuing CA also provides Certificate status information using a Repository in the form of a Certificate Revocation List (CRL) distribution point and/or Online Certificate Status Protocol (OCSP) responder.

1.3.2 Registration Authorities

The TrustFactory SSL Issuing CA acts as its own Registration Authority for certificates it issues.

An RA will be responsible for:

- Accepting, evaluating, approving or rejecting the registration of Certificate applications;
- Registering Subscribers for certification services;
- Providing systems to facilitate the identification of Subscribers (according to the type of Certificate requested);
- Using authorized documents or sources of information to evaluate and authenticate an Applicant's application;
- Requesting issuance of a Certificate via a multi-factor authentication process following the approval of an application; and
- Initiating the process to revoke, reissue, renew a Certificate from the applicable TrustFactory SSL Issuing CA.

Only Registration Authorities approved by the TrustFactory PA and that have signed the RA Agreement are permitted to submit requests to a TrustFactory Certification Authority for the issuance of Certificates.

1.3.3 Subscribers

A Subscriber, as used herein, refers to both the Subject of the Certificate and the entity that contracted with TrustFactory SSL Issuing CA for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant.

DNS Names may be listed as the subjectAltName extension of the following Certificate types:

- DomainPass Certificates
- DomainPass Premium Certificates
- DomainPass Wildcard Certificates
- OrganizationPass Certificates
- OrganizationPass Premium Certificates
- OrganizationPass Wildcard Certificates

Organization name may be listed as the Subject of the following Certificate types:

- OrganizationPass Certificates
- OrganizationPass Premium Certificates
- OrganizationPass Wildcard Certificates

1.3.4 Relying Parties

A Relying Party is a 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. A Relying Party may use information in the certificate to determine the suitability of the certificate for a particular use.

Relying Parties must always refer to TrustFactory SSL Issuing CA's revocation information either in the form of a CRL distribution point or an OCSP responder.

1.3.5 Other Participants

The CAs and RAs operating under the CP may require the services of other security, community, and application authorities. The CPS will identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.4 Certificate Usage

A Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1 Appropriate certificate usage

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

This CPS is applicable to the following Certificate types issued by the TrustFactory SSL Issuing CA:

- **TrustFactory DomainPass Certificates**

  These are SSL/TLS Domain Validated Certificates. They are typically used for server authentication and SSL/TLS secure sessions. SSL/TLS DV Certificates provide limited authentication of a Subscriber's server. The primary purpose of an SSL Certificate is to facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the Relying Party's internet browser and a Subscriber's secure server.

  Key Usage parameters are defined as:

  Key Usage:

  - Digital Signature
  - Key Encipherment

  Enhanced Key Usage:

  - Server Authentication

- Client Authentication

- **TrustFactory OrganizationPass Certificates**

  These are SSL/TLS Organisation Validated Certificates. They provide more trust than a SSL DV Certificates. Additional vetting of the organization is performed as well as the individual applying for the certificate. This might include checking the address where the company is registered and the name of a specific contact. This vetted company information is displayed to visitors on the certificate.

  Key Usage parameters are defined as:

  Key Usage:

  - Digital Signature
  - Key Encipherment

  Enhanced Key Usage:

  - Server Authentication
  - Client Authentication

- **DomainPass or OrganizationPass Premium Certificates**

  Both DomainPass and OrganizationPass Certificates are available as Premium certificates. The specified level domain is vetted and the certificate may be used for a total of five (5) sub-domains that contain the specified vetted level domain.

- **DomainPass or OrganizationPass Wildcard Certificates**

  Both DomainPass and OrganizationPass Certificates are available as Wildcard certificates. The specified level domain is vetted and the certificate may be used for an unlimited amount of sub-domains that contain the specified vetted level domain.

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 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.

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;
- where prohibited by law.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

TrustFactory Policy Authority
c/o iSolv Technologies
Rosebank Office Park, Block A, 1st floor,
181 Jan Smuts Avenue,
Parktown North

Johannesburg, 2163
South Africa
Tel: +27-11-880 6103
Fax: +27-11-880 5443
Email: info@trustfactory.net

1.5.2 Contact Person

Chairperson - TrustFactory Policy Authority
c/o iSolv Technologies
Rosebank Office Park, Block A, 1st floor,
181 Jan Smuts Avenue,
Parktown North
Johannesburg, 2163
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 Issuing 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 CA Browser Forum 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.

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 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 SSL 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.

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.

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).

Qualified Government Information Source: A database maintained by a Government Entity.

Qualified Government Tax Information Source: A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals.

Qualified Independent Information Source: A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.

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.

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
ARL	Authority Revocation List (A CRL for Issuing CAs rather than end entities)
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
EIR	Electric Industry Registry
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
LRA	Local Registration Authority
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)
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TLD	Top-Level Domain

TLS	Transport Layer Security
VAT	Value

2.0 Publication and Repository Responsibilities

2.1 Repositories

TrustFactory SSL Issuing CA publishes all CA Certificates, revocation data for issued Certificates, CP, CPS, and Relying Party agreements and Subscriber Agreements in Repositories at https://www.trustfactory.net/repository

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

2.2 Publication of Certificate Information

TrustFactory SSL Issuing 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.

TrustFactory SSL Issuing CA's Subscriber Certificate statuses are published in two formats:

1. The TrustFactory SSL Issuing CA Certificate Revocation List is accessible through the web-interface at: http://www.trustfactory.net/crl/tf-ssl-issuing.crl
2. The TrustFactory SSL Issuing CA Certificate Revocation List is accessible through an Online Certificate Status Protocol (OSCP) Responder at http://ocsp.trustfactory.net/tf-ssl-issuing

The Issuing 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.

TrustFactory SSL Issuing CA host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired and that chain up to each publicly trusted Root Certificate. The web pages are at the following url: www.trustfactory.net/test

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. Read-only access to the repository is unrestricted.

Logical and physical security measures are implemented to prevent unauthorized persons from adding, deleting, or modifying repository entries. The TrustFactory SSL Issuing CA ensures that the integrity and authenticity of its public documentation is maintained through the use of Digital Signatures applied to PDF documents.

3.0 Identification and Authentication

TrustFactory SSL Issuing CA will act as its own RA and authenticate and verify the attributes of the Applicant.

3.1 Naming

3.1.1 Types of Names

TrustFactory SSL Issuing 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 Subscriber to which the Subscriber Certificate is to be issued.

3.1.2 Need for Names to be Meaningful

The value of the common name attribute used in naming Subscribers shall contain the domain name or host name related to the web server or organization respectively.

3.1.3 Rules for Interpreting Various Name Forms

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

3.1.4 Uniqueness of Names

TrustFactory SSL Issuing 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 Subscriber.

3.1.5 Recognition, Authentication, and Role of Trademarks

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

3.2 Initial Identity Validation

TrustFactory SSL Issuing CA or authorized RAs may perform identification of the Applicant using any legal means of communication or investigation necessary to identify the Legal Entity or individual.

3.2.1 Method to Prove Possession of Private Key

Subscribers must prove possession of the Private Key corresponding to the Public Key being registered through a Certificate Signing Request (CSR) in PKCS#10 format.

This requirement does not apply where a key pair is generated by the TrustFactory SSL Issuing CA on behalf of a subscriber, for example where pre-generated keys are placed on smart cards.

3.2.2 Authentication of Organization Identity & Doman Identity

For all Certificates that include an organization identity, Applicants are required to provide the organization's name and registered or trading address. For all Certificates, the legal existence, legal name, assumed name, legal form (where included in the request or part of the legal name in the jurisdiction of incorporation) and requested address of the organization are verified using one of the following:

- A government agency in the jurisdiction of the Applicant, or a superior governing governmental agency if the Applicant claims they are a government agency themselves;
- A third party database that is periodically updated and has been evaluated by TrustFactory SSL Issuing CA to determine that it is reasonably accurate and reliable;
- An attestation letter confirming that Subject Identity Information is correct, written by a Commissioner of Oaths, Notary Public, or other reliable third party customarily relied upon for such information;
- An independent verification agency that operates in the jurisdiction in which the company is registered; or
- A site visit by the RA

3.2.2.1 Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain. The TrustFactory SSL Issuing CA validates each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

Note: For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

Note: FQDNs may be listed in Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

a) Domain Authorization Document

Confirming the Applicant's control over the requested FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication came from the Domain Contact.

The TrustFactory SSL Issuing CA verifies that the Domain Authorization Document was either (i) dated on or after the date of the domain validation request or (ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space.

b) Domain Ownership validation via email verification

Confirm the applicants control over the requested FQDN by emailing a verification email containing a verification link to the Domain Administrator as obtained from the WHOIS record for the domain.

c) Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS- ID, the TrustFactory SSL Issuing CA establishes and follows a documented procedure that determines if the wildcard character occurs in the first label position to the left of a “registry- controlled” label or “public suffix” (e.g. “*.com”, “*.co.uk”, see RFC 6454 Section 8.2 for further explanation).

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

TrustFactory SSL Issuing CA consults the "ICANN DOMAINS" section of an updated “public suffix list” such as http://publicsuffix.org/ (PSL). The PSL is updated regularly to contain new gTLDs delegated by ICANN, which are listed in the "ICANN DOMAINS" section.

For SAN validation each of the SAN domains will be individually verified as described in above section.

3.2.2.2 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the TrustFactory SSL Issuing CA evaluates the source for its reliability, accuracy, and resistance to alteration or falsification.

TrustFactory consults the following Reliable Data Source lists:

- the WHOIS records where applicable
- the http://publicsuffix.org/ “public suffix list” / ICANN DOMAINS

3.2.2.3 CAA Records

As part of the issuance process, the TrustFactory SSL Issuing CA checks for a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, according to the procedure in RFC 6844, following the processing instructions set down in RFC 6844 for any records found.

3.2.3 Authentication of Individual identity

TrustFactory SSL Issuing CA does not include the identity of a natural person in an SSL/TLS subscriber certificate.

3.2.4 Non Verified Subscriber Information

Information that is not verified shall not be included in certificates

3.2.5 Validation of Authority

Before issuing certificates that assert organizational authority, TrustFactory or the RA shall validate the authenticity of the Applicant Representative's certificate request and authority to act in the name of the organization.

A confirmation by telephone, confirmatory email, (using independently sourced telephone number and email) or comparable procedure to the Applicant Representative or with an authoritative source within the Applicant's organization (e.g. the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other appropriate department), to confirm certain information about the organisation, confirm that the organisation has authorised the certificate application, and confirm that the person submitting the certificate application on behalf of the certificate applicant is authorised to do so.

3.2.6 Criteria for Interoperation

Not applicable

3.3 Identification and Authentication for Renewal Requests

Certificate renewal requests must be authenticated.

TrustFactory SSL Issuing CA permits Certificate renewal prior to the expiry of the Subscriber's existing Certificate. Subscriber identity is established through log in to the Subscriber Management Portal and the current signature key is used to issue a CSR for the new certificate.

However identity shall be re-validated following the same procedures as the initial registration if 825 days has elapsed since the previous validation.

3.4 Identification and Authentication for Re-key/Re-issue Requests

TrustFactory SSL Issuing CA supports re-key or re-issue requests from Subscribers prior to the expiry of the Subscriber's existing Certificate.

- Re-key is only allowed for changing the Public key information on a certificate.
- Re-issue is only allowed for changing SAN details on a certificate.

In both cases the Expiry Date of the re-keyed/re-issued certificate remains the same as the current certificate. If any other certificate detail changes then a new certificate must be applied for.

3.4.1 Identification and Authentication for Routine Re-key/Re-issue

For re-key of any certificates issued by TrustFactory SSL Issuing CA, identity is established through the Subscriber Account credentials on the Subscriber Management Portal.

However identity shall be re-validated following the same procedures as the initial registration if 825 days has elapsed since the time of the previous validation.

3.4.2 Identification and Authentication for Re-key / Reissuance after Revocation

A routine re-key / re-issue after revocation is not supported. After a Certificate has been revoked, the Subscriber is required to go through the initial registration process described elsewhere 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 changed in any way, then the new certificate registration process must be followed and the identity proofing procedures outlined in this requirement must be re-performed and a new Certificate issued with the validated information.

TrustFactory SSL Issuing CA will not re-key a Certificate without additional authentication if doing so would allow the Subscriber to use the Certificate beyond the limits described above.

3.5 Identification and Authentication for Revocation Request

TrustFactory will accept revocation requests from:

1. The Subscriber, requested via the Subscriber Management Portal (login to the portal is acceptable authentication since it requires 2-factor authentication)
2. The TrustFactory operations team, after it is approved by the PKI Administrator

Revocation requests are granted after they are authenticated by TrustFactory SSL Issuing CA.

A revocation request may be communicated electronically if it is digitally signed with the Private Key of the Certificate Holder (or the Organisation, where applicable) requesting revocation.

Revocation requests received via email, at info@trustfactory.net, may be granted following a suitable challenge response as follows:

i. Upon receipt of a revocation request email, TrustFactory will send an email to the Subscriber email address supplied during registration, stating that the certificate will be revoked upon receiving a confirmation email message back from the Subscriber.

ii. Upon receipt of the confirming e-mail message back from the Subscriber, TrustFactory will revoke the Certificate.

4.0 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

For SSL/TLS certificates an Applicant may submit a certificate application to the TrustFactory SSL Issuing CA, by completing the application form on the TrustFactory website – www.trustfactory.net.
The Subscriber Management Portal on the TrustFactory website is the mechanism through which an Applicant / Subscriber submits New certificate requests, Renewal requests, Re-key/Re-issue requests and Revocation requests.

TrustFactory SSL Issuing CA maintains its own blacklists database of individuals from whom and entities from which it will not accept Certificate applications. The blacklist includes all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns.

The TrustFactory SSL Issuing CA checks for High Risk Certificate Requests and will not accept a certificate request if it is deemed High Risk.

4.1.2 Enrollment Process and Responsibilities

Applicants must submit sufficient information to allow TrustFactory SSL Issuing CA or the RA to successfully perform the required verification. TrustFactory SSL Issuing CA and RAs shall protect communications and securely store information presented by the Applicant during the application process in compliance with the TrustFactory Privacy Policy.

Generally, if the application is successful the enrolment process includes the following steps (but not necessarily in this order as some workflow processes generate Key Pairs after the validation has been completed):

- Agreeing to a Subscriber Agreement or other applicable terms and conditions; and paying any applicable fees.
- Submit a CSR from the Subscriber to the TrustFactory SSL Issuing CA;
- The TrustFactory SSL Issuing CA will validate and sign the Subscriber CSR and issue the Subscriber Certificate;
- Provide the Certificate back to the Applicant for installation.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Domain verification for SSL/TLS certificates shall be performed by the TrustFactory SSL Issuing CA. Applicant information MUST include, but not be limited to, at least one Fully-Qualified Domain Name to be included in the Certificate's SubjectAltName extension.

All communications sent through, either physical or electronic, are securely stored.

Once verification processes are completed, TrustFactory SSL Issuing CA shall retain all relevant information received in conformance with the requirements of the TrustFactory Privacy Policy and for a period of 7 years after the expiry or revocation of the Certificate.

4.2.2 Approval or Rejection of Certificate Applications

Assuming all verification steps can be completed successfully following the procedures in this CPS then TrustFactory SSL Issuing CA shall generally approve the Certificate Request. TrustFactory SSL Issuing CA may reject applications including for the following reasons:

- TrustFactory is unable to successfully verify the information provided by the Applicant.
- TrustFactory may reject requests based on potential brand damage to TrustFactory CAs in accepting the request.
- TrustFactory SSL Issuing CA may also reject applications for Certificates from Applicants who have previously been rejected or have previously violated a provision of their Subscriber Agreement, or are listed on the internal blacklist database or deemed High Risk.

TrustFactory SSL Issuing CA may not issue Certificates containing a new gTLD under consideration by ICANN unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name.

TrustFactory SSL Issuing CA is under no obligation to provide a reason to an Applicant for rejection of a Certificate Request.

4.2.3 Time to Process Certificate Applications

TrustFactory SSL Issuing CA shall ensure that all reasonable methods are used in order to evaluate and process Certificate applications within 7 working days. Where issues outside of the control of TrustFactory SSL Issuing CA occur, TrustFactory SSL Issuing CA shall strive to keep the Applicant duly informed.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

TrustFactory SSL Issuing CA can only accept certificate issuance requests from the Applicant directly. After satisfying itself that the verification checks have been successfully completed, the TrustFactory SSL Issuing CA may generate and digitally sign the Certificate applied for.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

TrustFactory SSL Issuing CA shall notify the Subscriber of the issuance of a Certificate at an email address which was supplied by the Subscriber during the enrollment process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

TrustFactory SSL Issuing CA shall inform the Subscriber that s/he may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. Unless the Subscriber notifies TrustFactory SSL Issuing CA within seven (7) days from receipt, the Certificate is deemed accepted.

4.4.2 Publication of the Certificate by the CA

TrustFactory SSL Issuing CA publishes the Certificate by delivering it to the Subscriber..

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No further notification to other entities is required..

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

TrustFactory SSL Issuing CA does not generate key pairs for subscribers. Subscribers must protect their Private Key taking care to avoid disclosure to third parties. TrustFactory SSL Issuing CA's Subscriber Agreement identifies the obligations of the Subscriber with respect to Private Key protection.

The Subscriber shall use its private key and the 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.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties must verify that the Certificate is valid by examining the CRL or OCSP Responders provided by TrustFactory SSL Issuing CA before initiating a transaction involving such Certificate.

TrustFactory SSL Issuing CA provides a Relying Party agreement to Subscribers, the content of which should be presented to the Relying Party. Relying Parties should check the status of the Certificate before relying on the Certificate and perform a risk assessment to ensure that their reliance is appropriate according to the defined key usage. Relying Parties must assess:

1. The appropriateness of the use of a Certificate for any given purpose and that it is not prohibited or otherwise restricted by this CPS.
2. That the certificate is being used in accordance with the KeyUsage field extensions included in

the certificate

3. The revocation status of the certificate and all the CAs in the chain that issued the certificate.

Software used by Relying Parties should be fully compliant with X.509 standards.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

TrustFactory SSL Issuing 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.
TrustFactory SSL Issuing CA will send an email notification to the Subscriber to renew a certificate at least 14 days before the expiry date.

4.6.2 Who May Request Renewal

TrustFactory SSL Issuing CA may accept a renewal request from the Subscriber provided that the renewal request is submitted and properly authenticated via the Subscriber Management Portal.
The CSR used should have the same Public Key to be certified as in the original certificate.

4.6.3 Processing Certificate Renewal Requests

Certificate Renewal requests do not require additional validation procedures as changes to certificate details are not allowed during renewal, except that identity shall be re-validated following the same procedures as the initial registration if 825 days has elapsed since the previous validation.

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal 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 / Re-issue

4.7.1 Circumstances for Certificate Re-Key

Subscribers may request routine re-key / re-issue.

TrustFactory SSL Issuing CA may re-key a Certificate as long as:

- The original Certificate to be re-keyed has not been revoked;
- The original Certificate to be re-keyed has not expired;
- The new Public Key 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 re-key is complete.

4.7.2 Who May Request Certification of a New Public Key

TrustFactory SSL Issuing CA may accept a re-key request provided that it is authorized by the original Subscriber, or an organization administrator who retains responsibility for the Private Key on behalf of a Subscriber.. A Certificate signing request is mandatory with any new Public Key to be certified. A re-key is

requested only via the Subscriber Management Portal

4.7.3 Processing Certificate Re-Keying / Re-issue Requests

TrustFactory SSL Issuing CA do not allow changes to certificate subject details during re-key. In the case of a re-key or reissuance, authentication through the Subscriber Management Portal is acceptable. A CSR is required for issuing the new certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.8 Certificate Modification

Modifying a certificate is not permitted. Subscribers should instead submit a request for new certificates.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Certificate revocation is a process whereby the serial number of a Certificate is effectively blacklisted by adding the serial number and the date of the revocation to a CRL. The CRL itself will then be digitally signed with the same Private Key which originally signed the Certificate to be revoked. Adding a serial number allows Relying Parties to establish that the lifecycle of a Certificate has ended. TrustFactory SSL Issuing CA may remove serial numbers when revoked Certificates pass their expiration date to promote more efficient CRL file size management. Prior to performing a revocation TrustFactory SSL Issuing CA will verify the authenticity of the revocation request.

Revocation of a Subscriber Certificate shall be performed within twenty-four (24) hours under the following circumstances:

1. The Subscriber requests by email or through the Subscriber Management Portal that TrustFactory CA operations revoke the Certificate;
2. The Subscriber notifies TrustFactory CA operations that the original certificate request was not authorized and does not retroactively grant authorization;
3. TrustFactory CA operations obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. TrustFactory CA operations obtains evidence that the Certificate was misused;
5. TrustFactory CA operations is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
6. TrustFactory CA operations 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);
7. TrustFactory CA operations is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
8. TrustFactory CA operations is made aware of a material change in the information contained in the Certificate;
9. TrustFactory CA operations is made aware that the Certificate was not issued in accordance with the Baseline Requirements or TrustFactory CA's Certificate Policy or Certification Practice Statement;
10. TrustFactory CA operations determines that any of the information appearing in the Certificate is inaccurate or misleading;
11. TrustFactory CA operations ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
12. TrustFactory SSL Issuing CA's right to issue Certificates under these Requirements expires or is

revoked or terminated, unless TrustFactory SSL Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;

13. TrustFactory CA operations is made aware of a possible compromise of the Private Key of the TrustFactory SSL Issuing CA used for issuing the Certificate;
14. Revocation is required by TrustFactory CA's Certificate Policy and/or Certification Practice Statement; or
15. 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).

Revocation of a Subscriber Certificate may also be performed within a commercially reasonable period of time under the following circumstances:

- TrustFactory SSL Issuing CA receives notice or otherwise become aware that the Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of TrustFactory SSL Issuing CA's jurisdiction of operation;
- Overdue payment of applicable fees by the Subscriber;
- Following the request for cancellation of a Certificate, if a Certificate has been reissued, TrustFactory SSL Issuing CA may revoke the previously issued Certificate;
- Under certain licensing arrangements, TrustFactory SSL Issuing CA may revoke Certificates following expiration or termination of the license agreement;
- TrustFactory SSL Issuing CA determines the continued use of the Certificate is otherwise harmful to the business of TrustFactory SSL Issuing CA or third parties. When considering whether Certificate usage is harmful to TrustFactory's or a third party's business or reputation, TrustFactory SSL Issuing CA will consider, among other things, the nature and number of complaints received, the identity of the complainant(s), relevant legislation in force, and responses to the alleged harmful use by the Subscriber;

4.9.2 Who Can Request Revocation

TrustFactory SSL Issuing CA shall accept authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the authorized RA, the Subscriber or an affiliated organization named in the Certificate. TrustFactory SSL Issuing CA may also at its own discretion revoke Certificates.

4.9.3 Procedure for Revocation Request

The primary method for requesting and authenticating revocation requests is through the Subscriber user account, on the Subscriber Management Portal.

Authentication of the revocation request from the Subscriber is done according to the process described in Section 3.5.

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

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.

The TrustFactory SSL Issuing CA 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 CA publicly discloses the instructions through its website at www.trustfactory.net.

TrustFactory SSL Issuing CA does not support bulk revocation.

4.9.4 Revocation Request Grace Period

Revocation requests shall be made as soon as reasonably practicable, but not more than 24 hours after detecting the loss or compromise of the Private Key.

4.9.5 Time Within Which CA Must Process the Revocation Request

TrustFactory SSL Issuing CA 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 (e.g. a law enforcement official); and
4. Relevant legislation.

TrustFactory SSL Issuing CA will revoke certificates as quickly as practical upon receipt of a proper revocation request. Section 4.9.1 states circumstances under which the revocation request will be processed within 24 hours and circumstances under which the revocation request will be processed within a commercially reasonable period of time.

Revocation requests shall be processed before the next CRL is published, excepting those requests received within twelve 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 or OCSP 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

TrustFactory SSL Issuing CA, that operates online, publishes CRLs at least every 24 hours and is valid for 7 days.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within 4 hours after generation.

4.9.9 On-Line Revocation Status Checking Availability

OCSP responses conform to RFC6960 and RFC5019. OCSP responses are either:
1. Signed by the SSL Issuing CA that issued the Certificates whose revocation status is being checked, or
2. Signed by an OCSP Responder whose Certificate is signed by the TrustFactory SSL Issuing CA that issued the Certificate whose revocation status is being checked. In this case, the OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

The TrustFactory SSL Issuing CA updates information provided via an Online Certificate Status Protocol at least every 24 hours and information is available to relying parties within 4 hours of CRL publication. OCSP responses from this service have a maximum expiration time of ten days.

4.9.10 On-Line Revocation Checking Requirements

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

The SSL Issuing 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 Issuing CA Private Key used to sign Subscriber Certificates, TrustFactory operations will as soon as practically possible inform the Subscriber 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 Subscriber Certificates

within 24 hours and publish online CRLs within 4 hours of creation and ARLs within 4 hours of creation.

4.9.13 Notification of Certificate Revocation to Subscriber

The TrustFactory SSL Issuing CA shall notify the Subscriber of the revocation of a Certificate using the email address submitted during the enrollment process

4.9.14 Circumstances for Suspension

Certificate suspension is not supported and not permitted. Subscribers should follow the Certificate Revocation procedures.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

TrustFactory SSL Issuing CA provides a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both. These services are presented to Relying Parties within the Certificate and may refer to any of the following URLs:

1. http://www.trustfactory.net/crl/tf-ssl-issuing.crl
2. http://ocsp.trustfactory.net/tf-ssl-issuing

Revocation entries on a CRL or OCSP Response are not be removed until after the Expiry Date of the revoked Certificate. CRLs and OCSP responses are signed by the TrustFactory SSL Issuing CA Private Key.

4.10.2 Service Availability

The TrustFactory SSL Issuing 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.

The TrustFactory SSL Issuing CA 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 Issuing 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 Issuing CA operates 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 all 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.

The TrustFactory SSL Issuing 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, 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 change in state of use
2. CA and Subscriber Certificate lifecycle management events, including:
   a. Certificate requests, renewal, and re-key requests, and revocation;
   b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
   c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
   d. Name of submitting RA,
   e. Acceptance and rejection of certificate requests;
   f. Issuance of Certificates;
   g. The subscriber's acceptance of the Subscriber Agreement; and
   h. Where required under privacy legislation, the Subscriber's consent to allow the TrustFactory to keep records containing personal data, pass this information to specified third parties, and publication of certificates.
   i. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
   a. Successful and unsuccessful PKI system access attempts;
   b. PKI and security system actions performed;
      - Actions taken by individuals in Trusted Roles;
      - Audit Log read or written;
      - Action taken against the Audit Log and security sensitive files

   c. Security profile changes;
   d. System crashes, hardware failures, and other anomalies; (MANUAL)
   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 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 valid business or security reasons, for any evidence of malicious activity and following each important operation.

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.

The records of events are date stamped in a secure manner that guarantees, from the date of creation of the record to the end of the archive period that there is a trusted link between the event and the time of its realisation.

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. If necessary, the audit collection system protects the data confidentiality. In the case of a problem occurring during the process of the audit collection TrustFactory determines whether to suspend TrustFactory SSL Issuing 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 Issuing CA performs regular vulnerability assessments covering all TrustFactory SSL Issuing 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 SSL Issuing CA 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 TrustFactory SSL Issuing CA retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

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

If a timestamping service is used to date the records, then it has to comply with the requirements defined in Section 6.8. Irrespective of timestamping methods, all logs must have data indicating the date and 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 Issuing CA archive information is checked upon creation. Only authorised TrustFactory SSL Issuing CA equipment, trusted role and other authorized persons are allowed to access the archive. Requests to obtain archive information are coordinated by people in trusted roles (the administrator, the manager. and the security officer).

5.6 Key Changeover

Towards the end of the SSL Issuing CA private key's lifetime, in accordance with Section 6.3.2, a new CA signing key pair is commissioned by the TrustFactory PA 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 Subscriber Certificates are maintained until such time as all Subscriber Certificates have expired.

Certificate Subject information may also be modified 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

5.7.1 Incident and Compromise Handling Procedures

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 Issuing CA was created during the initial start up of the CA application and is protected by the master keys for the TrustFactory SSL Issuing 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 Issuing CA generates all issuing Key Pairs in a physically secure environment by personnel in trusted roles under, at least, dual control. An external witness (ideally an independent auditor who normally performs audits on a regular basis) is present or the ceremony, as a whole, is videotaped/recorded. TrustFactory SSL Issuing CA key generation is carried out within a device which is certified at least to FIPS 140-2 level 3 or above.

6.1.2 Private Key Delivery to Subscriber

The Applicant shall be responsible for the generation and safeguarding of its private keys unless otherwise required and approved by the TrustFactory PA.

6.1.3 Public Key Delivery to Certificate Issuer

TrustFactory SSL Issuing CA only accepts Public Keys from Subscribers that are delivered to the TrustFactory SSL Issuing CA in a Certificate Signing Request (CSR) as part of the certificate application process.

6.1.4 CA Public Key Delivery to Relying Parties

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

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

6.1.5 Key Sizes

The TrustFactory SSL Issuing CA Certificate utilizes a key size of 4096 bits (RSA) with hash algorithm SHA-256.
Subscriber Certificates meet the following requirements for algorithm type and key size.

(1) Subscriber 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

CSSs 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 Issuing CA generates Key Pairs in accordance with FIPS 186 and uses reasonable techniques to validate the suitability of Public Keys presented by Subscribers, according to Baseline Requirements. Known weak keys shall be tested for and rejected at the point of submission.

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

TrustFactory SSL Issuing CA sets key usage and enhanced usage of Subscriber Certificates via the v3 Key Usage Field for X.509 v3 (see Section 7.1). Subscribers and Relying Parties shall only use Subscriber

Certificates in compliance with the TrustFactory SSL Issuing CA CPS and applicable laws.

TrustFactory SSL Issuing CA's Private Keys may be used for Digital Certificate signing and CRL and OCSP response signing. Keys may also be used to authenticate the TrustFactory SSL Issuing CA to a Repository. Refer to SSL Issuing CA Certificate Profile in Annexure A.

Refer to Section 1.4.1 for Key Usage parameters for the various Subscriber certificate types.

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 Issuing CA archives Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

TrustFactory end-entity Subscriber Certificates and renewed Certificates have a maximum Validity Period of 2 years.

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

6.4.3 Other Aspects of Activation Data

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

6.5 Computer Security Controls

Controls as per TrustFactory CP

6.6 Lifecycle Technical Controls

Controls as per TrustFactory CP

6.7 Network Security Controls

Controls as per TrustFactory CP

6.8 Time Stamping

Controls as per TrustFactory CP

7.0 Certificate, CRL, and OCSP Profiles

Typical content of information published on a TrustFactory SSL Certificate may include 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

7.1 Certificate Profile

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

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

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

Subscriber Certificates

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. keyUsage
Populated based on certificate type described in Section 1.4.1 and set in accordance with RFC 5280

e. extKeyUsage (required)
Populated based on certificate type described in Section 1.4.1 and set in accordance with RFC 5280

7.1.3 Algorithm Object Identifiers

No stipulation

7.1.4 Name Forms

TrustFactory SSL Issuing CA issues Certificates with name forms compliant to RFC 5280. By issuing a Subscriber Certificate, the TrustFactory SSL Issuing 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

7.1.5 Name Constraints

No stipulation

7.1.6 Certificate Policy Object Identifier

TrustFactory SSL Issuing CA issues certificates to Subscribers 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 Issuing CA issues Version 2 CRLs in compliance with RFC 5280. CRLs have the following fields:

- **Issuer:**
  CN = TrustFactory SSL Issuing 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 Issuing CA operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 2560 and RFC5019 and highlights this within the AIA extension via an OCSP responder URL.

7.3.1 Version Number(s)

TrustFactory SSL Issuing CA issues Version 1 OCSP responses with following fields:

- **Responder ID** SHA-1 Hash of responder's Public Key
- **Produced Time** the time at which this response was signed
- **Certificate Status** Certificate status referenced (good/revoked/unknown)
- **ThisUpdate/NextUpdate** Recommended validity interval for the response
- **Signature Algorithm** SHA256RSA
- **Signature** Signature value generated by the responder
- **Certificates** the OCSP responder's Certificate

An OCSP request must contain the following data:

- Protocol version
- Service request
- Target Certificate identifier

7.3.2 OCSP Extensions

No stipulation

8.0 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 Issuing 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 TrustFactory CP.

8.2 Identity/Qualifications of Assessor

Controls as per TrustFactory CP

8.3 Assessor's Relationship to Assessed Entity

Controls as per TrustFactory CP .

8.4 Topics Covered by Assessment

Controls as per TrustFactory CP.

8.5 Actions Taken as a Result of Deficiency

Controls as per TrustFactory CP.

8.6 Communications of Results

Controls as per 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 .

9.17 Other Provisions

Controls as per the TrustFactory CP

10 Annexure: SSL CA Certificate Profiles

10.1 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)