PUBLIC

TrustFactory Client Issuing CA Certification Practice Statement

05 November 2024

Version: 1.13

Shita
l Naik

Digitally signed
by Shital Naik
Date:
2024.11.05
12:44:14
+02'00'

Table of Contents

References and Acknowledgements

1.	CA / Browser Forum Network and Certificate System Security Requirements	http://www.cabforum.org
2.	CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	http://www.cabforum.org

1 Introduction

This Certification Practice Statement (CPS) applies to the products and services of TrustFactory Client Issuing CA. Primarily this pertains to the issuance and lifecycle management of Certificates including validity checking services. This CPS may be updated from time to time as outlined in Section 1.5, Policy Administration. 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 Digital Certificate is issued to a particular community and/or class of application with common security requirements". This CPS follows the content and structure guidance provided in Internet Engineering Task Force (IETF) RFC 3647, dated November 2003.

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

Where applicable in the context of individual or email certificates, TrustFactory Client Issuing CAs conform to the current version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and the Baseline Requirements, the Baseline Requirements take precedence over this document.

This CPS should be read together with the TrustFactory Certificate Policy. Certain practices, controls, compliance, business and legal matters that are common across all TrustFactory CAs are documented in the TrustFactory CP (and may not be repeated in this CPS – except to aid readability). This CPS addresses the specific technical and procedural practices of the TrustFactory Client Issuing CAs, within the TrustFactory PKI System, that issue Certificates to individuals.

1.1 Overview

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

- TrustFactory Client Issuing CA

The purpose of this CPS is to present the TrustFactory Client 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), this CPS and industry standards.

The Certificate subject names addressed in this CPS are the following:
CN = TrustFactory Client Issuing Certificate Authority
OU = TrustFactory PKI Operations
O = TrustFactory(Pty)Ltd
L = Johannesburg
S = Gauteng
C = ZA

1.2 Document Name and Identification

This document is the TrustFactory Client Issuing CA Certification Practice Statement (TrustFactory Client 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 its OID arcs for the various certificate and document objects as follows:

Document Objects Identifiers:

1.3.6.1.4.1.50318.1	TrustFactory CA CP
1.3.6.1.4.1.50318.2.2	TrustFactory Client Root CA Certificates Practice Statement
1.3.6.1.4.1.50318.2.4	TrustFactory Client Issuing CA Certificates Practice

Certificate Policy Object Identifiers:

1.3.6.1.4.1.50318.3.1	AATL compliant certificates
1.3.6.1.4.1.50318.3.2	SAAA AES compliant certificates

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

1.2.1 Document Revisions

Version	Description	Date
1.0	Initial for review	6 October 2017
1.1	Added certificate serial numbers and certificate profiles. Approved by Policy Authority	7 December 2017
1.2	Updates to Section 9.1 Fees Other minor corrections	15 December 2017
1.3	Key changes as follows: ▪ RAs must be approved by SAAA: 1.3.2 ▪ Added validation of DBA name: 3.2.2.2 ▪ Validate via video call: 3.2.3.2 ▪ Removed face-to-face validation via notary public: 3.2.3.3 ▪ TrustFactory does not validate OU field: 3.2.4 ▪ Removed revocation request via email: 3.5 ▪ RA's submit requests over API: 4.1.1 ▪ Provision to reuse validated documents: 4.2.1, 4.6.3 and 4.7.3 ▪ Notification of the status of certificate: 4.3.2 and 4.4.3 ▪ Cater for revocation in case of subscriber's death, being wound up or organization cease to exist: 3.5, 4.9.1 and 4.9.2 ▪ RA notification of revocation: 4.9.13 ▪ TrustFactory does not provide subscriber key management services: 6.1 ▪ CPS Amendments for AES certificates: 9.12 ▪ Added Product Certificate Profiles: 10.2, 10.3, 10.4 Other minor corrections to improve clarity, understanding and remove duplication	10 August 2018
1.4	Change to rectify typographical error in URL for CRL distribution points (sections 2.2, 4.10.1, 10.2, 10.3 and 10.4)	13 September 2018
1.5	Updates to incorporate latest CAB Forum changes on revocation requirements. Other minor corrections and clarifications.	21 November 2018
1.6	Key changes as follows: • Added Policy OIDs for AATL and AES certificates: 1.2 • Annual review and version numbering: 2.3 • Subscriber key generation and protection requirements: 6.1.1 and/ 6.1.2 • Explanation of EmailPass verification procedure: 3.2.3.1 • Clarified certificate problem reporting method: 4.9.2 and 4.9.3 Other minor corrections and clarifications.	20 March 2019
1.7	Updated to incorporate details as required by Mozilla Root Store Policy. Removed use of "no stipulation". Aligned subsection heading to RFC3647 / CAB Forum Baseline Requirements	31 March 2020
1.8	Minor corrections and clarifications	12 July 2021
1.9	Modifications to subscriber key generation and other minor clarifications in section 6.1 and 6.2	11 July 2022
1.10	Minor amendments to Sections 3.2.3.3 ; 4.2.2. and 4.9.2	03 April 2023
1.11	Minor amendments and clarifications to Sections 3.2.3.3; 4.1.1; 4.8 and 4.9.1.1	14 August 2024
1.12	Minor changes to Annexure A	10 September 2024
1.13	Minor changes to 3.2.3 and Annexure A	05 November 2024

1.3 PKI Participants

1.3.1 Certification Authorities

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

TrustFactory Client Root Certificate Authority
└ TrustFactory Client Issuing Certificate Authority
- ➢ PersonalPass Certificate
- ➢ PersonalPass Premium Certificate
- ➢ EmailPass Certificate

The TrustFactory Client Issuing CA is a Certification Authority that issues Certificates in accordance with this CPS. As a Certification Authority, TrustFactory Client Issuing CA performs functions related to Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation. TrustFactory Client 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.

The TrustFactory Client Issuing CA will also rely on approved external Registration Authorities (RAs) to conduct subscriber verification and registration.

1.3.2 Registration Authorities

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

TrustFactory Client Issuing CA makes its client certificate services available through authorized Registration Authorities (RA). An RA is 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;
- Requesting issuance of a Certificate via a strong authentication process following the approval of an application; and
- Initiating the process to revoke, reissue, and renew a Certificate from the applicable TrustFactory Client 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.

External RAs only identify, authenticate and verify Individuals applying for personal certificates. Verification of email control for email certificates will only be done by the TrustFactory system.

RAs that provide Advanced Electronic Signature Certificates are required to be approved by the South African Accreditation Authority.

1.3.3 Subscribers

Subscribers are natural persons or legal entities that successfully apply for and receive a Certificate to support their use in transactions, communications and the application of Digital Signatures.

A Subscriber, as used herein, refers to both the Subject of the Certificate and the entity that contracted with TrustFactory Client Issuing CA for the Certificate’s issuance.

Subscribers who are yet to be approved to be issued a certificate are Applicants.

Natural person’s names and address can be listed as the Subject of the following Certificate types:

- PersonalPass Certificates
- PersonalPass Premium Certificates

Email addresses can be listed as the Subject of the following Certificate types:

- EmailPass Certificates

1.3.4 Relying Parties

A Relying Party is a subordinate CA, person, entity, or organization that relies on or uses the TrustFactory Client 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 Client 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 identifies the parties responsible for providing such services, and the mechanisms used to support these services.

1.4 Certificate Usage

A client Certificate allows a person taking part in an electronic transaction to prove his/her 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 Client Issuing CAs.

1.4.1.1 TrustFactory EmailPass Certificates

Email Certificates are used by individuals to digitally sign and encrypt electronic messages via an S/MIME compliant application. The primary purpose of an Email Certificate is to provide authentication, message integrity, non-repudiation and privacy.

The assurance provided is as follows:

- Individual has demonstrated control of the email address that is the Subject of the certificate (other information provided on the application form is not verified).

Key Usage and Extended Key Usage parameters are as defined in the Certificate Profiles in Annexure A.

1.4.1.2 TrustFactory PersonalPass Certificates

Personal Certificates are used by individuals to digitally sign and encrypt electronic documents. These certificates are trusted by the Adobe Approved Trust List program. Personal Certificates help to provide authentication and document integrity.

The assurance provided is as follows:

- The individual name, that is the Subject of the certificate, is verified to a reasonable level of assurance against a certified copy of a valid government issued identity document (ID) such as passport, driver's license, or photo ID card.
- Individual has demonstrated control of the email address that is to be included in the certificate.

Key Usage and Extended Key Usage parameters are as defined in the Certificate Profiles in Annexure A.

1.4.1.3 TrustFactory PersonalPass Premium Certificates

Advanced Electronic Signature Certificates (AES Certificates) are compliant with the requirements of Advanced Electronic Signatures as prescribed by the ECT Act and are used by individuals to digitally sign and encrypt electronic documents or messages. The use of AES Certificates for digital signatures permits the authentication of the identity of correspondents, message integrity, and support for non-repudiation. Documents or messages signed with AES certificates can be used as evidence in a court of law in South Africa.

The assurance provided is as follows:

- The individual name, that is the Subject of the certificate, was present at a face-to-face meeting with the RA, or trusted agent and he/she hand-signed the subscriber agreement.
- The individual name, that is the Subject of the certificate, is verified to a reasonable level of assurance against an original valid government issued identity document (ID) such as passport, driver's license, or photo ID card.
- Individual has demonstrated control of the email address that is to be included in the certificate.

Key Usage and Extended Key Usage parameters are as defined in the Certificate Profiles in Annexure A.

1.4.2 Prohibited Certificate usage

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

Any usage of the Certificate inconsistent with these extensions is not authorized and shall be deemed prohibited usage. Certificates are not authorized 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

Any enquiry associated with this CPS should be addressed to:

TrustFactory Policy Authority
6th Floor, Firestation Rosebank
16 Baker Street
Rosebank
Gauteng, 2196
Republic of South Africa

Telephone:	+27 11 880-6103
Fax:	+27 11 880-5443
Email:	info@trustfactory.net

1.5.2 Contact Person

TrustFactory General Manager
6th Floor, Firestation Rosebank
16 Baker Street
Rosebank
Gauteng, 2196
Republic of South Africa

Telephone:	+27 11 880-6103
Fax:	+27 11 880-5443
Email:	info@trustfactory.net

Subscribers, Relying Parties, Application Software Suppliers, and other third parties can report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, through the "Report Abuse" link on the TrustFactory website at https://www.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 approves 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 Client 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

1.6.1 Definitions

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 (AES)
A specific digital signature that complies with the requirements of the Electronic Communications and Transactions (ECT) Act of 2002 in the Republic of South Africa, and can be relied upon as 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, written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Business Entity
Any entity that is not a Private Organization, Government Entity, or non-commercial entity. 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 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 (CA)

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 (CPS)

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

Certificate Signing Request (CSR)

A message or data sent to a CA or RA to request the issuance of a certificate.

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 (DNS)

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 (ECT) 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 "Not After" date in a Certificate that defines the end of a Certificate's Validity Period.

Fully-Qualified Domain Name (FQDN)

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

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)

A 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.

Internal Server Name

A server name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

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.

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.

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 (OCSP)

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 an office, 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.

Reliable Data Source

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

Reliable Method of Communication

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

Relying Party

Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such supplier merely displays information relating to a Certificate.

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. (https://www.trustfactory.net/repository).

Root CA

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

Root Certificate

The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subject

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

Subject Identity Information

Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the commonName field.

Subordinate CA

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

Subscriber

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

Subscriber Agreement

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

Technically Constrained Subordinate CA Certificate

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

Terms of Use

Provisions regarding the safekeeping and acceptable uses of a Certificate issued 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.

Validation Specialists

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

Validity Period

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

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 these 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.

WHOIS

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

Wildcard Certificate

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

X.509

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

1.6.2 Acronyms

AATL	Adobe Approved Trust List
AES	Advanced Electronic Signature

AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface
AOR	Authorized Organizational Representative
BR	CA/B Forum Baseline Requirements
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CSR	Certificate Signing Request
CRL	Certificate Revocation List
DNS	Domain Name System
DV	Domain Validation
EKU	Extended Key Usage
ERA	Enterprise Registration Authority
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
GST	General Sales Tax
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
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validation
PKI	Public Key Infrastructure
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
PA	Policy Authority
RA	Registration Authority
RFC	Request for Comments
SAAA	South African Accreditation Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VAT	Value Added Tax

2 Publication and Repository Responsibilities

2.1 Repositories

TrustFactory Client 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 Client Issuing CA may publish submitted information on publicly accessible directories for the provision of Certificate status information.

TrustFactory Client Issuing does not make certain classified and confidential documentation including business controls, operating procedures, security policies, processes and standards, and business continuity and recovery plans available to the public. These documents are, however, made available to Qualified Auditors as required during any WebTrust or SAAA audit performed on TrustFactory Client Issuing CA.

2.2 Publication of Certificate Information

TrustFactory Client Issuing CA publishes its CA Certificates, CP, CPS, and 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 Client Issuing CA's Certificate statuses are published in two formats:

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

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

2.3 Time or Frequency of Publication

The TrustFactory PA annually reviews this CPS and may make revisions and updates to policies as required by changes in the Requirements, 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 approved and digitally signed by the TrustFactory PA.

In order to reference that the annual review of this CPS has taken place, TrustFactory increments the version number and adds a dated changelog entry, even if no other changes are made to the document.

2.4 Access controls on repositories

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

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

3 Identification and Authentication

TrustFactory Client Issuing CA relies on authorized RAs to perform authentication of identities and verification of attributes of the Applicants. Where authentication and verification by the RA is successful then the RA may submit the CSR to the TrustFactory Client Issuing CA.

3.1 Naming

3.1.1 Types of Names

TrustFactory Client Issuing CA Certificates follow the X.500 distinguished names rules to identify a Subscriber. Common Names (CNs) respect name space uniqueness and are not misleading.

The common name is 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 for Client subscriber certificates will contain names with commonly understood semantics permitting the determination of the identity of the individual that is the subject of the certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

Distinguished names in Certificates are interpreted using X.500 standards and ASN.1 syntax. Rules for interpreting e-mail addresses are specified in RFC 2822.

3.1.5 Uniqueness of Names

TrustFactory Client 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.

3.1.6 Recognition, Authentication, and Role of Trademarks

TrustFactory Client Issuing CA may not use registered trademarks that infringe on the intellectual property rights of a third party, when assigning the distinguished names to Subscribers.

3.2 Initial Identity Validation

TrustFactory Client 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 by submitting a PKCS #10 Certificate Signing Request (CSR) signed using the Private Key.

3.2.2 Authentication of Organization Identity

3.2.2.1 Validation of Organization Identity

For all Certificates that are issued to an organization, 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; or
- A Reliable Data Source that has been approved by TrustFactory PA as being reasonably accurate and reliable; or
- 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; or
- An independent verification agency that operates in the jurisdiction in which the company is registered; or
- A site visit by the RA

The authority of the Applicant to request a Certificate on behalf of the organization is verified in accordance with Section 3.2.5 below

For certificates where the organization is an optional field, the applicant must provide TrustFactory with an affiliation letter prepared on an official organization letterhead, or similar that TrustFactory Validation Specialists deem to be reliable, confirming the applicant's affiliation with the organization

TrustFactory validates the affiliation through any of the following:

- A confirmation telephone call, (using independently sourced telephone number), or
- confirmatory email, (using independently sourced email address), or
- a comparable procedure that TrustFactory Validation Specialists deem to be reliable

with an authoritative source within the Applicant's organization (e.g., the human resource division, applicant's manager, information technology offices, or other appropriate department), to confirm certain information about the organization, confirm that the applicant is affiliated to the organization.

3.2.2.2 Use of Tradename or DBA name

For organizations that include a Tradename or DBS in the Certificate, TrustFactory verifies the Applicant's right to use the DBA/tradename using at least one of the following methods:

- Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
- A Reliable Data Source has been approved by TrustFactory PA as being reasonably accurate and reliable;
- Communication with a government agency responsible for the management of such DBAs or tradenames;
- An Attestation Letter accompanied by documentary support; or
- A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

3.2.2.3 Verification of Country

If the CountryName field is specified in the Certificate, then TrustFactory verifies the country of the Applicant using a proof of address such as utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that TrustFactory Validation Specialists determines to be reliable.

3.2.2.4 Validation of Domain Authorization or Control

Client Issuing CA certificates will not contain a Domain Name in the subject.

3.2.2.5 Authentication for an IP Address

TrustFactory does not permit listing IP Addresses in a Certificate.

3.2.2.6 Wildcard Domain Validation

Client Issuing CA certificates will not contain a Wildcard Domain Name in the subject.

3.2.2.7 Data Source Accuracy

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

3.2.2.8 CAA Records

Not applicable to the Client Issuing CA.

3.2.3 Authentication of Individual identity

TrustFactory RAs authenticate individuals depending upon the type of Certificate as indicated below. Additionally, the CA keeps record of the process that was followed for the issuance of each certificate

3.2.3.1 EmailPass Certificates

Individual has demonstrated control of the email address that is the Subject of the certificate as follows:

- TrustFactory uses an automated email challenge response process.
- TrustFactory sends an email that contains a verification link (which includes a random value) to the email address that is to be included in the subject (subjectAltName) of the certificate, and then receives a confirming response when the Applicant clicks on the verification link (utilizing the random value).

3.2.3.2 PersonalPass Certificates

The Applicant is required to submit a legible copy of a valid government issued photo identity document (ID) such as passport, driver's license, photo ID card or equivalent document type which matches the individual name, that is the Subject of the certificate.

The RA or authorized RA representative confirms the authenticity of the individual by means of a face-to-face meeting with the subscriber, or on a procedure that provides an equivalent assurance such as an online video recording. The individual must present their valid government issued photo ID document to the validation specialist for verification. The TrustFactory validation specialist inspects the document for legibility and authenticity.

The Applicant's address is verified against a valid utility bill, bank/financial statement or equivalent document which indicates the Applicant's physical address.

TrustFactory validates the Subject information using approved official or 3rd party data sources. If further assurance or verification is required, the applicant may be requested to submit a legally binding declaration of identity or other approved document fulfilling the requirement.

Individual has demonstrated control of the email address that is to be included in the certificate, as described in Section 3.2.3.1.

3.2.3.3 PersonalPass Premium Certificates

For initial registration

The Applicant is required to present an original valid government issued photo identity document (ID) such as passport, driver's license, photo ID card or equivalent document type which matches the individual name, that is the Subject of the certificate.

The RA or authorized RA representative, confirms the authenticity of the individual by means of a face-to-face meeting with the subscriber, or a procedure that provides an equivalent assurance such as an online video recording. The individual must present their valid government issued photo ID document to the validation specialist, and trusted agent for verification. The TrustFactory validation specialist and trusted agent inspects the document for legibility and authenticity.

In addition, the individual name, that is the Subject of the certificate, must physically present at an in person face-to-face meeting with the RA or authorized RA representative or trusted agent and submit a hand-signed subscriber agreement.

The Applicant's address is verified against a valid utility bill, bank/financial statement or equivalent document or through any other reliable means which indicates the Applicant's physical address.

TrustFactory validates the Subject information using approved official or 3rd party data sources. If further assurance or verification is required, the applicant may be requested to submit a legally binding declaration of identity or other approved document fulfilling the requirement.

Individual has demonstrated control of the email address that is to be included in the certificate, as described in Section 3.2.3.1.

For subsequent renewals, the individual name, that is the Subject of the certificate, must present at a face-to-face meeting ,or on a procedure that provides an equivalent assurance such as online video recording, and submit a signed subscriber agreement using their current valid AES certificate.

3.2.4 Non-Verified Subscriber Information

Not applicable as TrustFactory does not issue any certificates with unverified information.

3.2.5 Validation of Authority

Before issuing certificates that assert organizational authority, TrustFactory or the RA shall validate the subscriber's 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 organization, confirm that the organization has authorized the certificate application, and confirm that the person submitting the certificate application on behalf of the certificate applicant is authorized to do so.

An organization may provide TrustFactory with an Authority Letter that specifies the individuals who may request Certificates. TrustFactory verifies the Authority Letter and thereafter TrustFactory does not accept any certificate requests that are outside this specification. Other Applicants from the organization will be directed to the approved list of requestors.

3.2.6 Criteria for Interoperation

Not applicable. TrustFactory Client Root CA has not established any cross-certificates.

3.3 Identification and Authentication for Re-key Requests

TrustFactory Client Issuing CA supports re-key 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.

3.3.1 Identification and Authentication for Routine Re-key

For re-key of any certificates issued, the identity is authenticated through use of Subscriber Account credentials on the Subscriber Management Portal.

3.3.2 Identification and Authentication for Re-key after Revocation

A routine re-key after revocation is not supported. After a Certificate has been revoked, the Subscriber/RA is required to go through the initial registration and validation process described under Section 3.2 in this document to obtain a new Certificate.

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

3.4 Identification and Authentication for Revocation Request

TrustFactory accepts revocation requests from:

- The Subscriber, requested via the Subscriber Management Portal (login to the portal is acceptable authentication of the subscriber);
- The RA Administrator, requested via the RA application API or pre-determined trusted path;
- The TrustFactory operations team, after it is approved by the CA Administrator; or

- Duly authorized third parties may submit a request upon subscriber’s death, being wound up or organization cease to exist.

Revocation requests are granted after they are suitably authenticated and validated by the relevant TrustFactory RA.

4 Certificate Lifecycle Operational Requirements

4.0 Certificate Application

4.1.1 Who Can Submit a Certificate Application

TrustFactory Client Issuing CA may accept a new certificate application from:

- the Applicant directly via the TrustFactory website at www.trustfactory.net;
- an approved RA, provided that it is authorized by the original Applicant;
- a trusted authorized partner of the RA authorized by the applicant; or
- an organization administrator (Applicant Representative or
- an authorised representative who may retain responsibility for the Private Key on behalf of an applicant

The Subscriber Management Portal on the TrustFactory website, or the API are the mechanisms through which an Applicant / Subscriber submits new certificate requests as well as renewal requests, reissues, re-key and revocation requests.

Approved external RAs, trusted RA partners, trusted agents; or authorised representatives of the applicant, may submit certificate applications via a trusted path and is identified using strong authentication mechanisms (this is generally done over the secure API).

TrustFactory Client Issuing CA maintains its own blacklists database of individuals from whom, and entities from which, it does 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.

4.1.2 Enrollment Process and Responsibilities

Applicants must submit sufficient information to allow TrustFactory Client Issuing CA or the TrustFactory authorized RA to successfully perform the required verification. TrustFactory Client Issuing CA and RAs 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):

- Agreeing to a Subscriber Agreement and acceptance of other applicable terms and conditions;
- Paying any applicable fees;
- Submitting a CSR corresponding to the application; if an external RA is used then it submits the request via a trusted path and the RA is identified using strong authentication mechanisms;
- The TrustFactory Client Issuing CA validates the Subscriber CSR and certificate data submitted; and
- Issue the Subscriber Certificate and send a notification.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Initial identity verification for individual certificates are performed as set forth in Section 3.2. All information to be included in the Certificate must be supported with additional documents to enable the TrustFactory or authorized RA's validation specialists to verify the information.

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

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

TrustFactory may use the documents and data provided in Section 3.2 to verify certificate information, and may reuse previous validations themselves where applicable.

TrustFactory Client Issuing CA checks for High Risk Certificate Requests and do not issue new or replacement Certificates to an entity if it is deemed High Risk.

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 Client Issuing CA generally approve the Certificate Request.

TrustFactory Client Issuing CA reserves the right to reject applications based on any of the following reasons:

- TrustFactory Client Issuing CA is unable to successfully verify the information provided by the Applicant.
- TrustFactory Client Issuing CA may reject requests if there is a potential for negative consequences to TrustFactory's brand, reputation or operations in accepting the request.
- TrustFactory Client 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 Client Issuing CA, in its sole discretion, considers that the certificate will not be legally compliant for the intended use

TrustFactory Client 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 Client Issuing CA endeavours to process and evaluate Certificate applications within 30 days of receiving the application. Where delays are due to issues outside of TrustFactory's control, then TrustFactory will keep the Applicant informed.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

TrustFactory Client Issuing CA accepts certificate requests directly from the Applicant, through the Subscriber Management Portal, or from RAs approved by the TrustFactory PA, or through secure communication via API from RA trusted partners. TrustFactory Client Issuing CAs communicate with approved RAs and RA partners through a pre-established trusted path (generally this is over a secure API). TrustFactory Client Issuing CA only generate and digitally sign the Certificate applied for after all pre-requisite conditions have been met.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Notification of the status of certificate issuance is available to the Subscriber on the Subscriber Management Portal. TrustFactory Client Issuing CA will also send an email to the Subscriber directing him/her to access their account to retrieve the Certificate, using the email information submitted during the enrolment process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Subscriber is responsible for verifying the accuracy of the data incorporated into the Certificate. Unless the Subscriber notifies TrustFactory Client Issuing CA of any errors, within seven (7) days from issuance, the Certificate is deemed accepted, or the Certificate is deemed accepted upon first use.

4.4.2 Publication of the Certificate by the CA

TrustFactory Client Issuing CA publishes the Certificate by making it available to the Subscriber. Subscribers must log-in to the Subscriber Management Portal to access and download their certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Issuance status information is made available to external RAs, or RA trusted partners, if they were involved in the initial enrolment, over the software API, or through the subscriber portal should they be authorized to manage the subscriber account on behalf of the subscriber.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must protect their Private Key taking care to avoid disclosure to third parties. TrustFactory Client Issuing CA's Subscriber Agreement identifies the obligations of the Subscriber with respect to Private Key protection.

The Subscriber shall use his/her 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 indicated in the corresponding Certificate. Where it is possible to make a backup of a Private Key, Subscribers must use the same level of care and protection attributed to the live Private Key. At the end of the useful life of a Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup.

4.5.2 Relying Party Public Key and Certificate Usage

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

TrustFactory Client 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 to assess the risk and to ensure suitability of usage and assurances made prior to relying on the Certificate.

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 basic constraints, key usage and extended key usage 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

Certificate renewal requests are authenticated.
TrustFactory Client Issuing CAs permit Certificate renewal prior to the expiry of the Subscriber's existing Certificate. Subscriber identity is established through log in to the Subscriber Management Portal, or over API and the Subscriber submits a CSR containing the existing Public Key.

Identity is re-validated following the procedures under 3.2.3

TrustFactory Client Issuing CA may renew a Certificate under the following criteria:

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

The TrustFactory system automatically generates and send an email notifying the Subscriber of the need for renewal of a certificate, at least 28 days before the expiry date. The email is sent to the registered subscriber's email address.

4.6.2 Who May Request Renewal

TrustFactory Client Issuing CA may accept a renewal request from the Subscriber, an RA, an RA trusted partner, or an authorised representative of the subscriber, 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 renewal is requested via either login to the Subscriber Management Portal, or the RA's management system, or over secure API.

4.6.3 Processing Certificate Renewal Requests

Certificate Renewal requests do not generally require additional validation procedures as changes to certificate details are not allowed during renewal, except that identity will be re-validated following the procedures as mentioned under 3.2.3.
TrustFactory reuse previously validated documents, if they are still considered valid, to process the renewal request.

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

4.7.1 Circumstances for Certificate Re-Key

Subscribers may request routine re-key. TrustFactory Client Issuing CA may re-key a Certificate under the following criteria:

- The original Certificate to be re-keyed has not been revoked;
- The original Certificate to be renewed has not expired;
- The Subscriber 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 is revoked after re-key certificate is issued.

4.7.2 Who May Request Certification of a New Public Key

TrustFactory Client Issuing CA may accept a re-key request from the Subscriber or an RA, or RA trusted partner 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 re-key is requested via login to the Subscriber Management Portal, or over secure API or the RA’s management system.

A CSR is mandatory with any new Public Key to be certified.

4.7.3 Processing Certificate Re-Keying Requests

TrustFactory Client Issuing CA does not allow changes to certificate details during re-key. In the case of a re-key, authentication through the Subscriber Management Portal, or over secure APIs acceptable. A CSR is required for issuing the new certificate.

TrustFactory reuses previously validated documents, if they are still considered valid, to process the rekey request.

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 Certificate 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 / Re-issue

4.8.1 Circumstances for Certificate Modification

TrustFactory Client Issuing CA may modify/reissue a Certificate under the following criteria:

- The original Certificate has not been revoked;
- The Public Key from the original Certificate has not been blacklisted for any reason;
- The Subject details need to be modified and, or
- The subject detail email address field needs modification.

The original Certificate is revoked after the new certificate is issued.

4.8.2 Who May Request Certificate Modification

TrustFactory Client Issuing CA may accept a modification/re-issue request provided that it is authorized by the original Subscriber, or a RA, or RA trusted partner, or an AOR who retains responsibility for the Private Key on behalf of a Subscriber. A modification/re-issue request from the Subscriber is submitted via login to the Subscriber Management Portal or over secure API. A Certificate signing request is mandatory with any new Public Key to be certified. A modification/re-issue is requested via the Subscriber Management Portal, the RA Management System or over an API.

4.8.3 Processing Certificate Modification Requests

TrustFactory Client Issuing CA allows changes to certificate subject details or email address fields during modification/re-issue. In the case of a modification/re-issue, authentication through the Subscriber Management Portal, the RA Management System or over secure API, is acceptable. Email validation is performed on any email address that is modified.

TrustFactory reuse previously validated documents, if they are still considered valid, to process the modification/re-issue request.

Re-verification and Revalidation of Identity are performed 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 is followed and the identity proofing procedures for a new certificate outlined in Section 3.2. is re-performed and a new Certificate issued with the validated information.

4.8.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

As per 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

As per 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

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

1. The Subscriber requests through the Subscriber Management Portal that TrustFactory Client Issuing CA revoke the Certificate;
2. The Subscriber notifies TrustFactory Client Issuing CA 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.

Revocation of a Subscriber Certificate will be performed within five (5) days under the following circumstances:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. TrustFactory CA operations obtains evidence that the Certificate was misused;
3. 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;
4. TrustFactory CA operations is made aware of a material change in the information contained in the Certificate;
5. TrustFactory CA operations is made aware that the Certificate was not issued in accordance with the Baseline Requirements or the CA's Certificate Policy or Certification Practice Statement;
6. TrustFactory CA operations determines or is made aware that any of the information appearing in the Certificate is materially inaccurate;
7. TrustFactory Client Issuing CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
8. Revocation is required by the TrustFactory Client Issuing CA's Certificate Policy and/or Certification Practice Statement;
9. The TrustFactory CA operations is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/CLIENTkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed;
10. TrustFactory CA operations receives a certified copy of the subscriber's death certificate;
11. TrustFactory CA operations receives documentation that a subscriber that is a legal person has been wound up or registered or has ceased to exist (i.e., organization).
12. TrustFactory CA operations its sole discretion, considers the certificate not to be legally compliant for the intended use.

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

1. TrustFactory Client 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 Client Issuing CA's jurisdiction of operation;
2. Overdue payment of applicable fees by the Subscriber;
3. Under certain licensing arrangements, TrustFactory Client Issuing CA may revoke Certificates following expiration, termination, or breach of the license agreement;
4. TrustFactory Client Issuing CA determines the continued use of the Certificate is otherwise harmful to the business of TrustFactory Client Issuing CA or third parties. When considering whether Certificate usage is harmful to TrustFactory's or a third party's business or reputation, TrustFactory Client 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.
5. TrustFactory CA operations determines or is made aware that any of the information appearing in the Certificate may be inaccurate;

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

Not applicable.

4.9.2 Who Can Request Revocation

TrustFactory Client Issuing CA accepts revocation requests submitted via login to the Subscriber Management Portal or over secure API. A revocation request may be accepted from an organization administrator, RA trusted partner or AOR who retains responsibility for the Private Key on behalf of a Subscriber, or an affiliated organization named in the Certificate, or from an authorized RA. TrustFactory Client Issuing CA may also at its own discretion revoke Certificates. Individuals, who are duly authorized, may request revocation by sending relevant documentation in cases of subscriber's death, or a legal person has been wound up or registered or organization has ceased to exist.

Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports, through the "Report Abuse" link on the TrustFactory website at https://www.trustfactory.net. The individual reporting the certificate problem must provide their identity and contact details as well as the reasonable cause to revoke the certificate.

4.9.3 Procedure for Revocation Request

The primary method for requesting and authenticating revocation requests is through the Subscriber user account, via the online Subscriber Management Portal, or over secure API.

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

TrustFactory Client Issuing CA records 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 is added to the appropriate CRL. CRL reason codes may be included. CRLs are published according to this CPS.

Subscribers, Relying Parties, Application Software Suppliers, and other third parties can report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, through the "Report Abuse" link on the TrustFactory website at https://www.trustfactory.net.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which CA Must Process the Revocation Request

TrustFactory Operations will begin investigating Certificate Problem Reports within twenty-four (24) hours of receipt of the report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the TrustFactory CA operations will work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation will not exceed the time frames stipulated in Section 4.9.1.1. The date selected for revocation will consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint; and
5. Relevant legislation.

TrustFactory Client Issuing CA will revoke certificates as quickly as practical upon receipt of a proper revocation request. Section 4.9.1.1 states various circumstances under which the revocation request will be processed within either 24 hours or 5 days or within a commercially reasonable period of time.

Revocation requests will be processed before the next CRL is published, excepting those requests received within twelve hours of next CRL issuance.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties must validate the suitability of the Certificate to the purpose intended and ensure the Certificate is valid as well as each Certificate in the chain is valid. Relying Parties will need to consult the CRL or OCSP as referenced in each Certificate in the chain. Relying Parties must validate that the certificate chain itself is valid and in accordance with IETF PKIX standards.

PDF signing Certificates also require Relying Parties to check the status of the Adobe Root CRL. This CRL is outside the scope of this CPS but is located at http://crl.adobe.com/cds.crl.

4.9.7 CRL Issuance Frequency

TrustFactory Client 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 signed by an OCSP Responder whose Certificate is signed by the TrustFactory Client 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.

4.9.10 On-Line Revocation Checking Requirements

The TrustFactory Client 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.

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

The Client 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 requirements specified.

The TrustFactory Client Issuing CA shall notify the Subscriber of the revocation of a Certificate using the email address submitted during the enrolment process.

4.9.12 Special Requirements Related to Key Compromise

In the event of compromise of a TrustFactory Client 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 Client Root CA will revoke Issuing CA Certificates within 24 hours and publish the updated CRL within 24 hours of creation.

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

Not applicable. Certificate suspension is not supported and not permitted.

4.9.15 Procedure for Suspension Request

Not applicable. Certificate suspension is not supported and not permitted.

4.9.16 Limits on Suspension Period

Not applicable. Certificate suspension is not supported and not permitted.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

TrustFactory Client 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 the URLs to access the CRL and OCSP are provided in Section 2.2 of this CPS.

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

4.10.2 Service Availability

The TrustFactory Client 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 CA maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report (submitted via the Report Abuse link on the TrustFactory website), 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 requirements specified.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA Private Keys are never escrowed. TrustFactory Client Issuing CA does not offer key escrow services.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The TrustFactory CA hardware and software are hosted in a high security caged enclosure (the Vault) within a data center with strict physical security and access control procedures. The Vault barriers extend from real floor to real ceiling to prevent unauthorized access. The data center is made of concrete and steel construction.

5.1.2 Physical Access

5.1.2.1 Data Centres

TrustFactory CAs systems operate within secure data centers (vaults) that provide four layers of security to access sensitive hardware. A Closed-Circuit TV (CCTV) surveillance system, with motion activated digital recording is in place for the Vault. Only authorized personnel, contractors and vendors are allowed into the data center.

Access control is managed via an electronic access control system with biometric access control at the Vault entry/exit points. Two persons are required for access to the Vault. All successful access entry into the Vault is logged.

5.1.2.2 RA Operations Areas

TrustFactory's RA operations are protected against access from non-authorized individuals. Access to the building requires the use of an "access" card. Access card use is logged by the building security system. The TrustFactory offices are equipped with biometric access as well as video cameras. The support and vetting rooms are also access controlled. In the event of remote vetting, the operators make use of two factor authentication and VPN to access the TrustFactory RA software. Access logs and video records are reviewed on a regular basis. TrustFactory securely stores all removable media and paper containing sensitive information related to its CA or RA operations in secure lockers.

5.1.3 Power and Air Conditioning

TrustFactory CAs operate within a secure data center that is equipped with redundant power and cooling system. UPS and failover to power generator are in place in the event of power outage.

5.1.4 Water Exposures

TrustFactory CAs servers are located above ground and placed on raised flooring to protect against water leaks.

Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

TrustFactory CAs operate within a secure data center that is equipped with a fire detection and suppression system.

5.1.6 Media Storage

TrustFactory CAs ensure that any media used is securely handled to protect it from damage, and unauthorized access. Storage of backup media is kept off-site. All media containing sensitive data is securely disposed of when no longer required. Records are maintained of all removable media across their lifecycle.

Media containing private key material are stored in sealed tamper evident envelopes, within locked containers inside the Vaults.

Records are maintained of all removable media across their lifecycle (first received to destruction).

5.1.7 Waste Disposal

TrustFactory CA's ensure that paper documents and magnetic media containing sensitive or confidential information are securely disposed of by:

- in the case of magnetic media:
  - physical damage to, or complete destruction of, the asset;
  - the use of an approved utility to wipe or overwrite magnetic media; and
- in the case of printed material:
  - shredding, or destruction by an approved service.

5.1.8 Off-Site Backup

TrustFactory CAs performs routine backups of critical system data, audit log data, and other essential business information. The back-up facilities and procedures ensure that all essential business information, processes and software can be recovered following a disaster or storage media failure.

Back-up and recovery arrangements for individual systems are regularly tested to ensure that business continuity and disaster recovery plans are functional. Backup media are stored at a secure offsite location (at a location separate from the Certificate issuance equipment), with appropriate levels of physical and procedural security controls.

Transportation of backup tapes to/from the offsite storage facility are done using tamper-evident envelopes.

Backup and recovery procedures are documented in the TrustFactory operational procedures documents and the disaster recovery plan.

5.2 Procedural Controls

5.2.1 Trusted Roles

TrustFactory Trusted Persons include all employees, contractors, and consultants that have access to or control authentication and/or cryptographic operations. The trusted roles are distributed such that no single person can circumvent the security of the CA system. The functions performed in these roles form the basis of trust for all uses of the CA.

The operational trusted roles are the roles fulfilling the following functions:

- Validation Specialist / RA Operator:
  - responsible for approving issuance and revoking certificates
  - performs the Applicant/Subscriber information validation and verification duties

- Auditor:
  - reviewing of CA system audit logs
  - performing compliance checking of operational processes against the CP and CPS

- Security Officer:
  - overall responsibility for administering the CA's information security management system policies and processes
  - PKI systems asset management
  - key ceremony: script compliance, protection of key materials

- Systems Administrator:
  - installation, configuration and maintenance of the CA server and network systems
  - monitoring the operational health of CA systems
  - day-to-day operation, backup and recovery of CA systems
  - administration of the server operating systems and network components
  - preparing and physically operating the HSM appliance and related equipment (host server and attached workstations) for the key ceremony.
  - installing the server and HSM appliance into the vault after the ceremony.
  - Administrative duties on the HSM under a 2-person (dual custody) rule

- CA Administrator:
  - CA cryptographic key life cycle management functions
  - Setup and configuration of CA software
  - overall management and coordination of CA functions

Key Ceremony only trusted roles:

- HSM Administrator
  - administration of HSM under 2 of 3 rule
  - can be a backup/stand-in for the System Administrator with regards to operating the HSM appliance and related equipment

- Shareholder:
  - holder of a key share

- Normal Crypto User:
  - signing operations in key ceremony

Multiple people may hold the same trusted role, with collective privileges sufficient to fill the role. Other trusted roles may be defined in other documents, which describe or impose requirements on the CA operation.

The CA maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in trusted roles and makes them available during compliance audits. The RA maintains lists, including names, organizations, and contact information of those who act in RA Operations Staff, RA Administrators, and RA Security Officer roles for that RA.

5.2.2 Number of Persons Required per Task

TrustFactory CAs require multiple persons for critical CA tasks (e.g., Key Pair generation, backup and recovery) so that any malicious activity would require collusion. All participants shall serve in a trusted role as defined in Section 5.2.1 above.

The HSMs define a separation of roles for specific tasks, and in addition each role requires multi-person control as defined in the table below:

	ADMIN tasks	SHAREHOLDER tasks	USER tasks
Root CAs	2 of 3	3 of 5	1 of 1
Subordinate CAs	2 of 3	2 of 3	1 of 1
Issuing CAs	2 of 3	2 of 3	1 of 1

5.2.3 Identification and Authentication for Each Role

Before appointing a person to a trusted role, TrustFactory runs a background check for identity verification and criminal records.

For RA systems, trusted roles are authenticated using VPN and two-factor authentication.

For CA systems, smart card authentication is used to authenticate trusted roles.

5.2.4 Roles Requiring Separation of Duties

TrustFactory CAs enforce role separation either by the CA equipment or procedurally or by both means. Individual CA personnel are specifically designated to the trusted roles defined in Section 5.2.1 above and it is not permitted for any one person to serve in more than one operational trusted role at the same time.

No individual is assigned more than one identity when accessing CA equipment.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

TrustFactory CAs employ a sufficient number of personnel that possess the knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function.

Trusted roles and responsibilities are documented in job descriptions. The job descriptions include skills and experience requirements.

Personnel are appointed to become Trusted Persons based on a combination their background, qualifications, training or experience needed to perform their prospective job responsibilities competently and satisfactorily.

Managerial personnel are employed based on having experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities, and experience with information security, sufficient to carry out management functions.

5.3.2 Background Check Procedures

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the TrustFactory CA, TrustFactory verifies the identity and trustworthiness of such person.

All TrustFactory CA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA operations. The TrustFactory CA do not appoint to a trusted role any person who is known to have a conviction for a serious crime or another offence, if such conviction affects his/her suitability for the position.

Persons fulfilling Trusted Roles pass a background check, comprising identity verification and criminal record checks. CAs have a process in place to ensure employees undergo security background checks at least every 3 years.

5.3.3 Training Requirements

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

TrustFactory Validation Specialists are trained on the required tasks before they are allowed to perform their roles. Validation Specialists are required to pass an examination provided by TrustFactory on the information verification requirements outlined in the CPS's, to ensure that they possess the required knowledge and skills.

5.3.4 Retraining Frequency and Requirements

All personnel in Trusted Roles maintain skill levels consistent with the CA's training and performance programs. Individuals in trusted roles are aware of changes in the TrustFactory CA or RA operations, as applicable. Individuals are be retrained when any significant change to the operations is required.

Refresher training shall be conducted as and when required.

5.3.5 Job Rotation Frequency and Sequence

TrustFactory CAs should ensure that any change in the staff do not affect the operational effectiveness of the service or the security of the system.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

Contractor personnel employed in trusted roles are subjected to the same security controls, verification and training processes as permanent CA personnel.

TrustFactory verifies that each Delegated Third Party's personnel involved in the issuance of a Certificate meets the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

5.3.8 Documentation Supplied to Personnel

TrustFactory CAs make available this CP, corresponding CPS's, relevant policies, and operational documents to its employees in order for them to perform their duties.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files are 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, ceremony script, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits.

The TrustFactory Client 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,
        - Identity of the 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;
    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; and
    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;
    c. Security profile changes;
    d. System crashes, hardware failures, and other anomalies;
    e. Firewall and router activities; and
    f. Entries to and exits from the CA facility.

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

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

5.4.2 Frequency of Processing Logs

Audit logs are reviewed as follows:

1. the Security Officer reviews logs of security events on the IT & Security infrastructure on a weekly basis for any evidence of malicious activity.
2. the Internal Auditors review logs of certificate lifecycle management events as part of their ongoing internal audits.

Unauthorized or suspicious activity detected during the reviews is investigated.

5.4.3 Retention Period for Audit Log

Audit logs shall be 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.

5.4.4 Protection of Audit Log

The audit logs are protected in a manner to ensure they cannot be deleted or destroyed (except for transfer to long term media) for the duration of their retention period Only authorized trusted individuals are able to perform any operations, such as viewing, archiving or transfer to backup media, without modifying integrity, authenticity and confidentiality of the data. The records of events are date stamped in a secure manner. Digital signatures are used to protect the integrity of audit logs where applicable or required to satisfy legal requirements.

5.4.5 Audit Log Backup Procedures

Audit logs are backed up using online backup mechanism to the disaster recovery site, and at least once a month they are backed up to tape and taken to a vault for storage.

5.4.6 Audit Collection System (Internal vs. External)

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

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

TrustFactory CAs perform regular vulnerability assessments covering all TrustFactory CA systems related to Certificate issuance products and services.

TrustFactory CAs undergo a penetration test on the CA's Certificate Systems on at least an annual basis and after significant infrastructure or application upgrades or modifications.

TrustFactory requires that each Delegated Third Party (or RA) also perform similar vulnerability assessments and penetration tests on their Certificate systems.

Additionally, the TrustFactory'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 complies with all record retention policies that apply by law and are retrieved as necessary by request of authorized parties.

5.5.2 Retention Period for Archive

The TrustFactory CAs and Delegated Third Parties (or RAs) retain all documentation relating to certificate requests and the verification thereof, and all Certificates issued 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

Archive records are stored at a secure location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction.

5.5.4 Archive Backup Procedures

Archive data is backed up over the network to storage media within the DR data center vault. Backup tape media are then transferred to an offsite storage vault.

Paper records are transferred to a secure storage facility that is access controlled and waterproof (e.g., a safe).

5.5.5 Requirements for Timestamping of Records

Irrespective of timestamping methods, all logs have data indicating the date and time at which the event occurred.

5.5.6 Archive Collection System (Internal or External)

All archive records are collected from internal systems and processes.

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing of TrustFactory CA archive information are checked upon creation. Only authorized TrustFactory CA equipment, trusted roles and other authorized persons are allowed to access the archive.

Requests to obtain archive information shall be coordinated by people in trusted roles (the system administrator, the general manager, and the security officer).

5.6 Key Changeover

Towards the end of the Client 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

TrustFactory handles incident and compromise according to incident response and management procedures that aim to minimize the impact of such events.

The incident management procedures include an assessment to determine if the CA or RA system needs to be rebuilt, if only some Certificates need to be revoked, and/or if a CA hierarchy needs to be declared as Compromised. Management will determine when it is appropriate to invoke the disaster recovery plan.

TrustFactory has a documented business continuity plan and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The TrustFactory CAs annually test, review, and updates these procedures.

The business continuity plan includes:
1. The conditions for activating the plan
2. Emergency procedures
3. Fallback procedures
4. Resumption procedures
5. A maintenance schedule for the plan

6. Awareness and education requirements
7. The responsibilities of the individuals
8. Recovery time objective (RTO)
9. Regular testing of contingency plans
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken
14. The distance of recovery facilities to the CA's main site
15. Procedures for securing its facility to the extent possible during the period of time following a disaster. TrustFactory does not publicly disclose its business continuity plans but make its business continuity plan and security plans available to the CA's auditors upon request

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

TrustFactory CAs have established incident management procedures that outline the steps to be taken if computing resources, software, and/or data are corrupted or suspected to be corrupted, or compromised.

If any equipment is damaged or rendered inoperative, but the Private Keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate Certificate status information according to the TrustFactory CA's disaster recovery plan.

5.7.3 Entity Private Key Compromise Procedures

In the event a TrustFactory CA Private Key is Compromised, lost, destroyed or suspected to be Compromised, the following procedures shall be followed after investigation of the problem:

1. The trust anchor managers and relying parties, should be notified within 6 hours to remove the self-signed certificates from their trust stores.
2. All the Subscribers who have been issued a Certificate will be notified at the earliest feasible opportunity, but within 24 hours.
3. If the PKI system can be securely re-established, then new Root CA or Issuing CA certificates shall be generated.

5.7.4 Business Continuity Capabilities after a Disaster

The TrustFactory operational processes deal with the business continuity for all TrustFactory CAs after a disaster, such as natural disasters, system outages, security incidents and compromise. A disaster recovery hot-standby site is in place to provide for timely recovery of CA services in the event of a system outage or disaster and provide continuity of operations.

The DR site is a suitable distance away from the production site, so that the DR site is not affected by an external incident which impacts the production site.

Certificate status information systems are deployed so as to provide 24 hours per day, 365 days per year availability.

5.0 CA or RA Termination

The TrustFactory Policy Authority is the body authorized to terminate a TrustFactory Root CA or TrustFactory Issuing CA for any reason whatsoever.

In the event of termination of a TrustFactory CA or RA, the TrustFactory CA shall provide 90 days' notice to all customers prior to the termination and certificates will be revoked at the end of the 90 day notice period.

In addition, the CA will:

- Stop delivering Certificates according to and referring to this CP or the relevant CPS
- Revoke the CA certificates
- Archive all audit logs and other records prior to termination
- Destroy all Private Keys upon termination
- Ensure archive records are transferred to an appropriate authority to be determined at the time by the TrustFactory Policy Authority, such as another TrustFactory CA that delivers identical services

- Use secure means to notify customers and software platform providers to delete all trust anchors
- Notify relevant regulatory authorities that require reporting of termination

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The signing key pair for the TrustFactory Client Issuing CA is protected by the master keys for the TrustFactory Client 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 Client Issuing CA generates its CA Key Pairs under the following conditions:

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

6.1.1.2 RA Key Pair Generation

Not applicable.

6.1.1.3 Subscriber Key Pair Generation

For Subscriber key generation facilitated by TrustFactory, Key generation is performed in a secure cryptographic device that meets FIPS 140-2 (or equivalent) using key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6.

Subscribers/Applicants are required to ensure that:

1. Key pairs are generated within a secure cryptographic hardware device that is compliant with the FIPS140-2 Level 2 standard, and under the control and possession of the Subscriber/Applicant; or
2. Where a cloud based service is used, the cloud based key generation takes place within a FIPS140-2 Level 2 hardware security module and that activation processes are based on 2-factor authentication of the Subscriber/Applicant; and
3. The key length and algorithm must meet the criteria for subscriber certificates as defined in Section 6.1.5.

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.

The key generator must ensure that all reasonable precautions are taken to prevent any loss, disclosure, or unauthorized use or modification of the private key during the generation, secure transfer and storage into the Subscriber's/Applicant's secure cryptographic hardware device.

Where a cloud based service is used, then the key activation and access must rely on at least a 2-factor authentication process and no duplication and export of the private key is permitted, except for documented service availability purposes.

The Subscriber/Applicant must take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token).

6.1.3 Public Key Delivery to Certificate Issuer

TrustFactory Client Issuing CA only accepts Public Keys from Subscribers that are delivered to the TrustFactory Client Issuing CA in a PKCS#10 Certificate Signing Request (CSR) as part of the certificate application process.

6.1.4 CA Public Key Delivery to Relying Parties

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

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

6.1.5 Key Sizes

The TrustFactory Client Issuing CA 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:

Subscriber Certificates (including infrastructure certificates):

Digest algorithm	SHA- 256, SHA-384 or SHA- 512
RSA modulus size (bits)	Minimum 2048 bits and must be divisible by 8
ECC curve	NIST P-256 or P-384

6.1.6 Public Key Parameters Generation and Quality Checking

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

6.1.7 Key Usage Purposes

TrustFactory Client Issuing CA sets key usage and extended key usage of Subscriber Certificates via the key usage fields for X.509 v3 Certificates (see Section 7.1).

Subscribers and Relying Parties shall only use Subscriber Certificates in compliance with the TrustFactory Client Issuing CA CPS and applicable laws.

TrustFactory Client 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 Client Issuing CA to a Repository. Refer to Client Issuing CA Certificate Profile in Annexure A.

Key Usage and Extended Key Usage parameters for the various Subscriber certificate types are defined in the Certificate Profiles in Annexure A.

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

TrustFactory Root and Issuing CAs ensure that all systems signing Certificates and CRLs or generating OCSP responses use FIPS 140-2 level 3 as the minimum level of cryptographic protection.
TrustFactory Issuing CAs that require Subscribers to use FIPS 140-2 level 2 or above systems for Private Key protection contractually obligate the Subscriber to use such a system or provide a suitable mechanism to guarantee protection.

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

The CA Private Key activation, use and backup operations require multi-person control as follows:

CA	Shareholder Control	HSM Administrator Control
Root CA	3 of 5	2 of 3
Subordinate CA	2 of 3	2 of 3
Issuing CA	2 of 3	2 of 3

6.2.3 Private Key Escrow

TrustFactory Root and Issuing CAs do not escrow CA Private Keys.

6.2.4 Private Key Backup

TrustFactory's Private Keys are generated and operated inside a cryptographic module, which has been evaluated to at least FIPS 140-2 Level 3. Two backups are created. One backup is stored at the primary site and one backup at the DR site.

Key Backups are created as part of the key generation ceremony procedure.

6.2.5 Private Key Archival

Parties other than the TrustFactory Issuing CA shall not archive the Issuing CA Private Keys without authorization by the TrustFactory Policy Authority.

TrustFactory Root and Issuing CAs do not archive Private Keys after expiry.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All keys are generated by and in a cryptographic module. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form.

TrustFactory Root and Issuing CA Private Keys are generated, activated and stored in Hardware Security Modules. Private Key transfer into or from a cryptographic module is performed in secure manner under multi-person control.

Private Keys must never exist in plain text outside of a cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

TrustFactory CAs stores CA Private Keys on at least FIPS 140-2 level 3 Hardware Security Modules. Root Private Keys are stored offline in cryptographic modules or on backup tokens as described in 6.2.2, 6.2.4 and 6.2.6. Issuer CA private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8 Method of Activating Private Key

TrustFactory Private Keys are activated according to the specifications of the cryptographic module manufacturer. Subscribers are solely responsible for protecting their Private Keys. Subscribers should use a strong password or equivalent authentication method and should also take measures for the physical protection of their workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

6.2.9 Method of Deactivating Private Key

When a TrustFactory Root/Issuing CA is no longer operational, its Private Keys are removed from the Hardware Security Module, which is then powered down and kept physically secured.

6.2.10 Method of Destroying Private Key

TrustFactory CA Private Keys are destroyed when they are no longer needed or when the Certificate to which they correspond have expired or are revoked.

TrustFactory CA personnel shall destroy the CA Private Key (including all associated CA secret activation data, as well as backups of Private Keys) by deleting and overwriting the key data via HSM re-initialization or zeroization, or physical destruction with a metal shredder or hammer. Such destruction shall be documented and witnessed.

The TrustFactory PA must authorize any CA Private Key destruction.

6.2.11 Cryptographic Module Rating

Cryptographic modules are certified to FIPS 140-2 level 3. See Section 6.2.1.

For offline CAs (the TrustFactory Root CAs) the cryptographic hardware is verified on a periodic basis. The hardware is verified by powering up the Root CA HSM and running diagnostics at least once per annum.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

TrustFactory Client Issuing CA archives Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

TrustFactory Client 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 3 years.

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

All TrustFactory personnel are instructed to memorize and not to write down their password or share it with another individual. TrustFactory locks accounts used to access secure CA processes if a certain number of failed password attempts occur as specified in the internal security policies, procedures.

6.4.3 Other Aspects of Activation Data

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

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Computer security technical requirements are achieved utilizing a combination of hardened system software configurations, operating system security features, malicious code protection on user workstations, firewalls and intrusion prevention systems on the network and physical safeguards.

The TrustFactory CA PKI components include the following functions:

- Require authenticated logins for trusted role;
- Enforce multi-factor authentication for all accounts capable of directly causing certificate issuance;
- Provide discretionary access control;
- Provide security audit capability (protected integrity);
- Generate and archive audit records for all transactions; and
- Require use of cryptography for session communication.

The computer systems are configured with the minimum of the required accounts and network services enabled.

6.5.2 Computer Security Rating

No stipulation.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

The system development controls for the TrustFactory CA are as follows:

- The system software is licensed from the vendor, no development or modification is done by TrustFactory.
- System software is released by the vendor with a crypto hash that can be used to verify the integrity of the software prior to installation. (This requirement does not apply to commercial off-the-shelf hardware or software).
- TrustFactory has a quality assurance process that is applied to all software updates and patches.
- The CA system is implemented and tested in a non-production environment prior to implementation in a production environment.
- No change is made to the production environment unless the change has gone through the TrustFactory Change Control process.
- All hardware will be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
- Hardware and software updates are purchased in the same manner as original equipment; and are installed by trusted and trained personnel following defined procedures.

6.6.2 Security Management Controls

The configuration of the TrustFactory CA system as well as any modifications and upgrades are documented and controlled by the TrustFactory CA management. The TrustFactory CA software, when first loaded, is checked as being that supplied from the vendor, with no modifications, and is the version intended for use.

6.6.3 Lifecycle Security Controls

TrustFactory Information Security Management System provides the security policies, standards and processes to ensure a trustworthy secure environment.

Only applications required to perform the CA operations are installed on the equipment and are obtained from trusted sources.

All software used is kept up to date according to vendor requirements.

Anti-virus software running on the workstations is automatically kept up to date.

6.7 Network Security Controls

TrustFactory CA and RA functions are performed using networks secured in accordance with the standards documented in the TrustFactory CP to prevent unauthorized access, tampering and denial of service attacks. Communications of sensitive information is protected using point to point encryption for confidentiality and digital signatures for non-repudiation and authentication.

TrustFactory documents and controls the configuration of its systems, including any upgrades or modifications made. TrustFactory CA system is connected to one internal network and is protected by firewalls and Network Address Translation for all internal IP addresses.

Customer validation and support and workstations are also protected by firewall(s) and only use internal IP addresses. Root Keys are kept offline and brought online only when necessary to sign Certificate-issuing subordinate CAs, OCSP Responder Certificates, or periodic CRLs. Firewalls are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

TrustFactory blocks all ports and protocols and opens only ports necessary to enable CA functions.

All unused network ports and services are disabled. TrustFactory’s network configuration is reviewed on-site by its auditors under an appropriate non-disclosure agreement.

6.8 Time Stamping

TrustFactory Root CAs do not use a time stamp service. Manual procedures are be used to maintain system time.

All TrustFactory Issuing CA (online CA) components are regularly synchronized with a Network Time Protocol (NTP) service. A dedicated authority, such as a timestamping authority, may be used to provide this trusted time.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Typical content of information published on a TrustFactory Client 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

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

Certificate profiles are provided in Annexure A.

7.1.1 Version Number(s)

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

7.1.2 Certificate Content and Extensions

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

7.1.2.1 Root Certificate

Not applicable.

7.1.2.2 Subordinate CA Certificate

Not applicable.

7.1.2.3 Subscriber Certificates

certificatePolicies	This extension is not set as critical. certificatePolicies:policyIdentifier is populated as per the profile in annexure A.
cRLDistributionPoints	This extension is not set as critical, and it contains the HTTP URL of the CA's CRL service.
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).
keyUsage	Populated based on certificate type described in Section 1.4.1 and set in accordance with RFC 5280
extkeyUsage (required)	Populated based on certificate type described in Section 1.4.1 and set in accordance with RFC 5280

7.1.2.4 All Certificates

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

7.1.3 Algorithm Object Identifiers

TrustFactory complies with all the current baseline requirements with regards to this section 7.1.3. including 7.1.3.1 and 7.1.3.2

TrustFactory issues Certificates with algorithms indicated by the following OIDs:

SHA256WithRSAEncryption	{ iso(l) member-body(2) us(840) rsadsi (113549) pkcs(l) pkcs-l(l) 11 }
SHA384WithRSAEncryption	{ iso(l) member-body(2) us(840) rsadsi (113549) pkcs(l) pkcs-l(l) 12 }
SHA512WithRSAEncryption	{ iso(l) member-body(2) us(840) rsadsi (113549) pkcs(l) pkcs-l(l) 13 }

TrustFactory does not currently sign Certificates using the RSA with PSS padding.

TrustFactory currently do not have any CAs signing certificates using ECDSA keys.

7.1.4 Name Forms

7.1.4.1 Issuer Information

TrustFactory Client Issuing CA issues Certificates with name forms compliant to RFC 5280 and the current baseline requirements stipulated under section 7.1.4.

7.1.4.2 Subject Information – Subscriber Certificates

By issuing a Subscriber Certificate, the TrustFactory Client Issuing CA represents that it followed the procedure set forth in this CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

For EmailPass certificates, the extension subjectAltName contains subject's full email address.

7.1.5 Name Constraints

Not applicable. TrustFactory Client Issuing CA is not considered technically constrained.

7.1.6 Certificate Policy Object Identifier

TrustFactory Client 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 requirements specified.

7.1.8 Policy Qualifiers Syntax and Semantics

No requirements specified.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No requirements specified.

7.2 CRL Profile

7.2.1 Version Number(s)

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

Issuer :	CN = TrustFactory Client 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 Client Issuing CA operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 6960 and RFC5019 and highlights this within the AIA extension via an OCSP responder URL.

7.3.1 Version Number(s)

TrustFactory Client Issuing CA issues Version 1 OCSP responses.

7.3.2 OCSP Extensions

TrustFactory Client Issuing CA issues 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

8 Compliance Audit and Other Assessments

TrustFactory CA ensures that it:

1. Issues Certificates and operates its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with the Baseline Requirements (as applicable to Client certificates);
3. Comply with the audit requirements set forth in this section; and
4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

The TrustFactory CAs have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced. CAs are audited for compliance to the current applicable version of the one or more of the following standards:

- WebTrust for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
- South African Accreditation Authority – ECT Act Regulations

Authorized RAs that provide Advanced Electronic Signature Certificates are required to be audited for compliance to South African Accreditation Authority requirements.

TrustFactory complies with the South African National Consumer Protection Act (CPA) requirements.

8.1 Frequency and Circumstances of Assessment

TrustFactory CAs complete a compliance audit to ensure compliance with the WebTrust or SAAA standards identified above (where products and services offered require compliance) via a Qualified Auditor on an annual basis at least. The audits are divided into an unbroken sequence of audit periods that do not exceed one year in duration.

8.2 Identity/Qualifications of Assessor

Applicable audits of TrustFactory CAs are performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme such as stipulated in section 8.0 of this document;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third- party attestation function;
- Licensed by WebTrust;
- Bound by law, government regulation, or professional code of ethics; and
- Maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

TrustFactory selects auditor(s)/assessor(s) who are completely independent from the TrustFactory CA.

8.4 Topics Covered by Assessment

The audit meets the requirements of the following audit scheme:

- WebTrust for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
- CA Browser Forum Baseline requirements
- South African Accreditation Authority – ECT Act Regulations (where applicable)

Authorized RAs that provide Advanced Electronic Signature Certificates are required to be audited for compliance to South African Accreditation Authority requirements.

An audit scheme will be applicable to the TrustFactory CA in the year following the adoption of the updated scheme.

For Delegated Third Parties, which are not Enterprise RAs, the TrustFactory CA shall obtain an audit report, issued under the above auditing standards, that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the TrustFactory CA's Certificate Policy and/or Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then the TrustFactory CA shall not allow the Delegated Third Party to continue performing delegated functions.

8.5 Actions Taken as a Result of Deficiency

If presented with a material non-compliance by external auditors, TrustFactory CAs shall create a suitable corrective action plan to remove the deficiency. Corrective action plans which directly affect policy and procedure as dictated by the CP and CPS are referred to the TrustFactory Policy Authority.

If required by the applicable supervisory authority or accrediting body, the material non-compliance and corrective action will be reported to the relevant body.

8.6 Communications of Results

Results of the audit are reported to the TrustFactory Policy Authority and also the General Manager for analysis and resolution of any deficiency through a subsequent corrective action plan.

Where required, the results of audits on TrustFactory CAs and authorized RAs are also communicated to the relevant standards bodies (WebTrust or SAAA).

All TrustFactory CA audit reports are also published on the Repository.

8.7 Self-Audits

TrustFactory CA monitors adherence to its Certificate Policy and Certification Practice Statements and strictly controls its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least two percent of the Certificates issued.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

TrustFactory charges fees for the issuance, management and renewal, of the various Certificate products that it offers. Such fees are provided on the TrustFactory website (www.trustfactory.net) and presented to Subscribers at the time the service is consumed.

TrustFactory reserves the right to change its fee structure from time to time without prior notice to Subscribers.

9.1.2 Certificate Access Fees

TrustFactory reserves the right to charge a fee for access to its databases of issued Certificates.

9.1.3 Revocation or Status Information Access Fees

TrustFactory does not charge a fee for access to its published CRLs or OCSP services as described in the applicable CA's CPS. However, reserves the right to charge a fee for providing customized CRLs, OCSP services, or other value-added services related to revocation and status information services.

9.1.4 Fees for Other Services

TrustFactory CAs reserves the right to charge a fee for other additional services not described in this CP or in a CPS.

9.1.5 Refund Policy

TrustFactory Issuing CAs will cancel and refund, or issue a store credit, for a certificate order upon request by a customer within 30 days of the original purchase. The refund/cancellation request must be made via the Customer's account on the TrustFactory Subscriber Management Portal, or via email to TrustFactory.

In the event a certificate is purchased for fraudulent use, the product and associated payment are forfeited and the customer does not qualify for a refund or exchange of any kind. If the certificate was issued, it will be canceled without any notice or permission.

Subscribers who choose to invoke the refund policy will have all respective issued Certificates revoked.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

TrustFactory maintains a Professional Indemnity insurance policy to cover claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining Certificates.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End Entities

TrustFactory Issuing CAs offer a Warranty Policy published on TrustFactory Repository at https://www.trustfactory.net/repository.

9.3 Confidentiality of Business Information

TrustFactory CAs treat personal information provided by Applicants/Subscribers as being confidential information and therefore are subject to protection by TrustFactory CA staff to avoid wrongful public disclosure.

In addition the following information is also confidential and not for public disclosure:

- Audit logs from CA and RA systems;
- Internal TrustFactory CA operational policy, standards and process documentation and business performance information
- Audit Reports from internal and independent auditors
- All commercial agreements and financial records
- Any TrustFactory information classified as Internal or Confidential

9.3.1 Scope of Confidential Information

TrustFactory CAs treat personal information provided by Applicants/Subscribers as being confidential information and therefore are subject to protection by TrustFactory CA staff to avoid wrongful public disclosure.

9.3.2 Information Not Within the Scope of Confidential Information

Any information not listed as confidential is considered public information. Published Certificate and revocation data is considered public information.

9.3.3 Responsibility to Protect Confidential Information

TrustFactory CAs protect confidential information. TrustFactory CAs protect confidential information through its information security polices, standards and processes and through training and contracts with employees, agents and contractors.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

TrustFactory CAs protect personal information in accordance with the TrustFactory Privacy Policy published in the Repository at https://www.trustfactory.net/repository.

9.4.2 Information Treated as Private

TrustFactory CAs treat all information received from Applicants that is not included in a Certificate or a CRL, as private. This applies to information from unsuccessful Applicants.

9.4.3 Information Not Deemed Private

Certificate status information, including reasons for revocation, and any Certificate content is deemed not private.

9.4.4 Responsibility to Protect Private Information

TrustFactory CAs PKI participants, including RAs, receiving private information protect it in accordance with the published Privacy Policy and prevent compromise and disclosure to third parties, whilst ensuring compliance with all local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to Use Private Information

Personal information is to be used in accordance with this CP, the CPS and the Privacy Policy. TrustFactory CAs include any required consents in the Subscriber Agreement, including permission required for any additional information to be obtained from third parties that may be applicable to the product or service being offered by the TrustFactory CA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

TrustFactory CAs may disclose private information, subject to applicable privacy laws, in cases where:

- disclosure is necessary in response to subpoenas and search warrants.
- disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.
- required to do so by law or regulation or order of a court of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property rights

TrustFactory CAs does not knowingly violate the intellectual property rights of third parties. Public and Private Keys remain the property of Subscribers who legitimately hold them. TrustFactory CAs retain ownership of Certificates and revocation information that they issue, however they shall grant permission to reproduce and distribute Certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, TrustFactory's root public keys and the root Certificates containing them, including all self-signed Certificates, are the property of TrustFactory. TrustFactory licenses software manufacturers to reproduce such root Certificates to place copies in trustworthy software.

TrustFactory owns all intellectual property rights in and associated with its logos, databases, web sites, digital Certificates, trade names, copyrights, software, processes and systems, training manuals, operating manuals, materials distributed to RA, RA associates, applicants and others as promotional material and any other publication originating from TrustFactory including this CP, and all TrustFactory CA CPS documents.

TrustFactory and the TrustFactory logo are the registered trademarks of TrustFactory.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

TrustFactory CAs use this CPS and applicable Subscriber Agreements to convey legal conditions of usage of issued Certificates to Subscribers and Relying Parties. Participants that may make representations and warranties include TrustFactory CA, RAs, Subscribers, Relying Parties, and any other participants as it might become necessary. All parties including the TrustFactory CA, any RAs and Subscribers warrant the integrity of their respective Private Key(s). If any such party suspects that a Private Key has been Compromised they will immediately notify the appropriate RA.

TrustFactory CA represents and warrants to Certificate Beneficiaries, during the period when the Certificate is valid, TrustFactory CA has complied with its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate:

- **Right to Use Domain Name or IP Address**: That, at the time of issuance, TrustFactory CA implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's Subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in TrustFactory CA's Certificate Policy and/or Certification Practice Statement (see Section 3.2);

- **Authorization for Certificate:** That, at the time of issuance, TrustFactory CA implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in TrustFactory CA's Certificate Policy and/or Certification Practice Statement (see Section 3.2.5);

- **Accuracy of Information:** That, at the time of issuance, TrustFactory CA implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in TrustFactory CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);

- **No Misleading Information:** That, at the time of issuance, TrustFactory CA implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in TrustFactory CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);

- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA implemented a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in TrustFactory CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);

- **Subscriber Agreement:** That, if TrustFactory CA and Subscriber are not Affiliates, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the Baseline Requirements, or, if TrustFactory CA and Subscriber are Affiliates, the Applicant Representative acknowledged and accepted the Terms of Use (see Section 4.5.1);

- **Status:** That TrustFactory CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and

- **Revocation:** That TrustFactory CA will revoke the Certificate for any of the reasons specified in its Certificate Policy.

- **Fiduciary relationship:** TrustFactory CAs are not the agents, fiduciaries, trustees, or other representatives of subscribers or relying parties.

9.6.2 RA Representations and Warranties

RAs warrant that:

- Verification and Issuance processes are in compliance with this CP and the relevant TrustFactory CA CPS;

- All information provided to TrustFactory CA does not contain any misleading or false information; and

- All translated material provided by the RA is accurate.

- The RAs are not the agents, fiduciaries, trustees, or other representatives of subscribers or relying parties.

- The RA maintains the ability to ensure:
  a) the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  b) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  c) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational security measures; and
  d) compliance with applicable data protection legislation.

It complies with all applicable statutory obligations and liabilities, including legislations governing labour and employment, safety of personnel and property, data protection legislation and taxation

9.6.3 Subscriber Representations and Warranties

Subscribers and/or Applicants, of end-entity certificates, warrant that:

- Subscriber will provide accurate and complete information at all times to TrustFactory CA, both in the Certificate Request and as otherwise requested by TrustFactory CA in connection with issuance of a Certificate;

- Subscribers and/or Applicant shall take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key to be included in the requested Certificate(s) and any associated activation data or device, e.g. password or token;

- Subscriber shall review and verify the Certificate contents for accuracy;

- For Client Certificates, the Subscriber shall use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;

- Subscriber shall (a) promptly request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate; and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;

- Subscriber shall promptly cease use of Private Key associated with the Public Key in the Certificate upon revocation of that Certificate;

- Subscriber shall respond to TrustFactory CA's instructions concerning Compromise or Certificate misuse within forty-eight (48) hours; and

- Applicant acknowledges and accepts that TrustFactory CA is entitled to revoke the Certificate immediately if the Applicant violates the terms of the Subscriber Agreement or Terms of Use or if TrustFactory CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

For TrustFactory Issuing CA Certificates that are signed by a TrustFactory Root CA the TrustFactory PA ensure that:

- Information in the Issuing CA Certificate is accurate and complete before publishing it to the Repository;

- All reasonable measures are taken to assure control of, keep confidential, and properly protect at all times the Private Key of the Issuing CA and any associated activation data or device, e.g. password or token;

- The Certificate contents are verified for accuracy;

- The Certificate is used in compliance with all applicable laws and in accordance with this CP and The applicable CA's CPS;

- The Issuing CA Certificate is, within 24 hours, revoked and use of its associated Private Key is terminated, if:
  i. there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in Certificate; and
  ii. if any information in the Certificate is or becomes incorrect or inaccurate;

9.6.4 Relying Party Representations and Warranties

A party relying on a TrustFactory CA's Certificate warrants to:

- Have the technical capability to use Certificates;

- Receive notice of the TrustFactory CA and associated conditions for Relying Parties;

- Validate a TrustFactory CA's Certificate by using Certificate status information (a CRL or OCSP) published by the TrustFactory CA in accordance with the proper Certificate path validation procedure;

- Trust a TrustFactory CA's Certificate only if all information featured on such Certificate can be verified via such a validation procedure as being correct and up to date;

- Rely on a TrustFactory CA's Certificate, only as it may be reasonable under the circumstances; and

- Notify the appropriate TrustFactory CA or RA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been compromised.

The obligations of the Relying Party, if it is to reasonably rely on a Certificate, are to:

- Verify the validity or revocation of the CA Certificate using current revocation status information as indicated to the Relying Party;

- Take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or this CP;

- Take any other precautions prescribed in the TrustFactory CA's Certificate as well as any other policies or terms and conditions made available in the application context a Certificate might be used.

Relying Parties must at all times establish that it is reasonable to rely on a Certificate under the circumstances taking into account circumstances such as the specific application context a Certificate is used in.

Claims, by Relying Parties, of liability for misuse of the certificate on excluded applications will be disallowed and the Relying Party will be notified by email of the disallowance of such claims.

9.6.5 Representations and Warranties of Other Participants

No Stipulation.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, TrustFactory CA disclaim all warranties, including any warranty of merchantability or fitness for a particular purpose, outside the context of the TrustFactory Warranty Policy.

TrustFactory CA does not warrant:

1. the accuracy of any unverifiable piece of information contained in Certificates except as it may be stated in the relevant product description,
2. the accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo Certificates.

9.8 Limitations of Liability

In no event shall TrustFactory CA be liable for any indirect, incidental, special or consequential damages or for any loss of profits, loss of data or other indirect incidental, consequential damages arising from or in connection with the use, delivery, reliance upon, license, performance or non-performance of certificates, digital signatures or any other transactions or services offered or contemplated by this CPS or the relevant CA CP.

In no event shall TrustFactory CA be liable for any acts of God, or other party's responsibilities, or any liability incurred if the fault in the verified information on a certificate is due to fraud or wilful misconduct of the Applicant, or any liability that arises from the usage of a certificate that has not been issued or used in conformance with the TrustFactory CP and CPS, or any liability that arises from security, usability, integrity of products, including hardware and software a Subscriber uses, or Any liability that arises from compromise of a Subscriber's private key.

In no event shall TrustFactory or any resellers or co-marketers, or any subcontractors, distributors, agents, suppliers, employees or directors of any of the foregoing be liable to any applicants, subscribers or relying parties or any other third parties for any losses, costs, liabilities, expenses, damages, claims or settlement amounts arising from or relating to claims of infringement, misappropriation, dilution, unfair competition or any other violation of any patent, trademark, copyright, trade secret or any other intellectual property or any other right of person, entity or organization in any jurisdiction arising from or relating to any certificate issues by a TrustFactory CA or arising from or relating to any services provided in relation to a certificate issued by a TrustFactory CA.

To the extent TrustFactory CA has issued and managed the certificate in accordance with this CPS and the relevant CA CP (Note: The baseline requirements for Publicly Trusted S/MIME certificates are excluded from TrustFactory's CP and CPS), TrustFactory CA shall not be liable to the subscriber, relying party or any third parties for any losses suffered as a result of use or reliance on such certificate. Otherwise outside of the context of the TrustFactory warranty policy, the TrustFactory CA's liability to the subscriber, relying party or any third parties for any such losses shall in no event exceed the cost of the certificate.

This liability cap limits damages recoverable outside of the context of the TrustFactory warranty policy. Amounts paid under the warranty policy are subject to their own liability caps.

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber agreements.
The liability (and/or limitation thereof) of enterprise RA's and the applicable CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 Indemnities

9.9.1 Indemnification by TrustFactory CA

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the TrustFactory CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the TrustFactory Root CA do not assume any obligation or potential liability of the TrustFactory CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others.

TrustFactory CA shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the TrustFactory CA, regardless of the cause of action or legal theory involved.

This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the TrustFactory CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the TrustFactory CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify TrustFactory CA, its partners, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CPS, or applicable law; (iii) the Compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence; or (iv) Subscriber's misuse of the Certificate or Private Key.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify TrustFactory CA, its partners, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10 Term and Termination

9.10.1 Term

This CPS remains in force until such time as communicated otherwise by TrustFactory CA on its web site or Repository.

9.10.2 Termination

The TrustFactory CP and CPSs as amended from time to time shall remain in force until they are replaced by a new version. Notified changes are appropriately marked by an indicated version. See Section 9.12 for Amendments procedures and notification.

9.10.3 Effect of Termination and Survival

TrustFactory CAs communicate the conditions and effect of termination of the CP and any of their Root CAs CPS's or Issuing CAs CPS's via their Repository.

9.11 Individual Notices and Communications with Participants

TrustFactory accepts notices related to this CP and any of its Root CAs CPS's or Issuing CAs CPS's by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from TrustFactory CA the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows.

Individuals communications made to TrustFactory must be addressed to email info@trustfactory.net or by post to TrustFactory in the address provided in Section 1.5.2.

9.12 Amendments

With respect to Advanced Electronic Signature certificates, significant changes are defined as changes that impact on the:

- identification process
- reliance limits of certificates
- key generation, storage and usage

In compliance with the regulations of the ECT Act in relation to Advanced Electronic Signature certificates, TrustFactory will submit a notification of the significant changes and updated edition in writing to the South African Accreditation Authority and notify relying parties and subscribers by publishing a notice of intention to effect change on the Repository, at least 30 days prior to the changes taking effect.

9.12.1 Procedure for Amendment

The TrustFactory Policy Authority review and approve any amendments to this CP or a CA's CPS. For changes deemed to have significant impact on the TrustFactory CA's users, an updated edition of this CP or a CA's CPS are published to the TrustFactory Repository within ten days of being approved by the PA.

Revisions not denoted "significant" are those deemed by the TrustFactory Policy Authority to have minimal or no impact (such as clerical changes) on Subscribers and relying parties using Certificates and CRLs issued by a TrustFactory CA. Such revisions may be made without notice to users of this CP or a CA's CPS and without changing the version number of the CP / CPS.

The TrustFactory Policy Authority has the sole authority to determine whether an amendment to the CP / CPS requires a version numbering change.

Controls are in place to reasonably ensure that the CP / CPS is not amended and published without the prior authorization of the TrustFactory Policy Authority.

The updated CP or CPS is published in the TrustFactory Repository at www.trustfactory.net

9.12.2 Notification Mechanism and Period

TrustFactory PA provides notice of an amendment to this CP or a CA's CPS by posting the revised CP / CPS to the Repository on the TrustFactory website. Following publication of the amended CP and CPS, changes become effective and are deemed accepted immediately upon publication, except where a specific notification period is required by a regulatory body then a notice will be placed on the Repository stating the date by when the revised CP or CPS is deemed accepted and effective.

With specific regard to the TrustFactory Client Issuing CA CPS, changes will be notified to the SAAA at least 30 days prior to implementation, and the changes are deemed accepted and effective 30 days after publishing the CPS to the Repository.

9.12.3 Circumstances Under Which OID Must be Changed

The TrustFactory Policy Authority has the sole authority to determine whether an amendment to the CP / CPS requires an OID change.

9.13 Dispute Resolution Provisions

Where contractual agreements are in place with third parties, the dispute shall be resolved pursuant to provisions in the contractual agreements.

For disputes arising under, in connection with or relating to this CP or a TrustFactory CPS, complaining parties agree to notify TrustFactory of the dispute in an effort to seek dispute resolution, before resorting to any other resolution mechanism including adjudication, mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice. The Parties shall, at the first instance, attempt to resolve all disputes through discussion in an atmosphere of mutual cooperation. TrustFactory management will respond to a formal dispute notice within 30 days.

In the event of failure to mutually resolve the dispute, the dispute shall be referred to arbitration or an Independent Technical Expert (if the dispute is of a technical nature). The Arbitrator or Independent Technical Expert shall be chosen by the parties by mutual agreement. If the Parties cannot agree on an Arbitrator or Independent Technical Expert, then the dispute shall be finally resolved in accordance with the rules of the Arbitration Foundation of Southern Africa applicable to international arbitration by an arbitrator appointed by the Foundation. In the event that the parties do not agree to the seat, the Foundation will select the seat of the arbitration.

The decision of such an arbitrator shall be binding on the partners.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of the Republic of South Africa shall govern the enforceability, construction, interpretation, and validity of this CP and of all TrustFactory CA CPSs, irrespective of contract or other choice of law provisions. This choice of law is made to ensure uniform procedures and interpretation for all participants, no matter where they are located.

Each party, including TrustFactory CA partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Gauteng, South Africa.

9.15 Compliance with Applicable Law

TrustFactory complies with applicable laws of the Republic of South Africa.

Export of certain types of software used in certain TrustFactory CA public Certificate management products and services may require the approval of appropriate public or private authorities. Parties (including TrustFactory CAs, Subscribers and Relying Parties) agree to comply with applicable export laws and regulations as pertaining in Republic of South Africa.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The TrustFactory CA will contractually obligate every CA and RA involved with Certificate issuance to comply with this CPS. No third party may rely on or bring action to enforce any such agreement.

9.16.2 Assignment

Entities operating under this CPS must not assign their rights or obligations without the prior written consent of TrustFactory.

Where TrustFactory has provided written consent to assign rights and obligations detailed in this CPS and an associated TrustFactory CA CP (including as a result of merger or a transfer of a controlling interest in voting securities), such assignment should be undertaken consistent with this CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties.

9.16.3 Severability

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

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

TrustFactory may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. TrustFactory's failure to enforce a provision of this CPS does not waive TrustFactory's right to enforce the same provisions later or right to enforce any other provisions of this CPS. To be effective any waivers must be in writing and signed by TrustFactory.

9.16.5 Force Majeure

TrustFactory is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond TrustFactory's reasonable control. The operation of the Internet is beyond TrustFactory's reasonable control.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting TrustFactory.

9.0 Other Provisions

TrustFactory is subject to the jurisdiction and regulatory framework of the Republic of South Africa. TrustFactory's CA infrastructure is based in South Africa. TrustFactory's sales offices and/or strategic partners have no access to any part of TrustFactory's CA infrastructure. TrustFactory will use all reasonable legal defense against being compelled by a third party to issue Certificates in violation of this CPS and associated TrustFactory CA CP.

10 Annexure A: Client CA Certificate Profiles

10.1 TrustFactory Client Issuing CA – Certificate Profile

V1 Fields	
Version	V3
Serial number	
Signature algorithm	sha256RSA
Signature hash algorithm	sha256

Issuer	CN = TrustFactory Client Root Certificate Authority
	OU = TrustFactory PKI Operations
	O = TrustFactory(Pty)Ltd
	L = Johannesburg
	S = Gauteng
	C = ZA

Validity	15 years

Subject	CN = TrustFactory Client 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=0
Key Usage	Digital Signature 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-client-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-client-issuing.crl
Properties	
Thumbprint algorithm	SHA1

10.2 EMAILPASS CERT PROFILE

EMAILPASS	**V1 Fields**
Version	V3
Serial number	
Signature algorithm	sha256RSA
Signature hash algorithm	sha256

Issuer	CN = TrustFactory Client Issuing Certificate Authority
	OU = TrustFactory PKI Operations
	O = TrustFactory(Pty)Ltd
	L = Johannesburg
	S = Gauteng
	C = ZA

Validity	*1 , 2 or 3 years*
Subject	*emailAddress=*
Public key	RSA (*minimum 2048 bits*)
Extensions	
Basic Constraints	Subject Type=EndEntity
	Path Length Constraint=None
Key Usage	Digital Signature Key Encipherment
Enhanced key usage (property)	None
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-client-issuing [2] Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= https://www.trustfactory.net/repository/tf-online-client.crt
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.50318.2.4 [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-client-subscriber.crl
SubjectAltName	*emailAddress*
Properties	
Thumbprint algorithm	SHA1

10.3 PERSONALPASS CERT PROFILE

PERSONALPASS	**V1 Fields**
Version	V3
Serial number	
Signature algorithm	sha256RSA
Signature hash algorithm	sha256

Issuer	CN = TrustFactory Client Issuing Certificate Authority
	OU = TrustFactory PKI Operations
	O = TrustFactory(Pty)Ltd
	L = Johannesburg
	S = Gauteng
	C = ZA

Validity	*1, 2 or 3 years*

Subject	CN = *first name and surname*
	OU = *(optional)*
	O = *(optional)*
	L = *(optional)*
	ST = *(optional)*
	C = *country*
	emailAddress=

Public key	RSA (*minimum 2048 bits*)
Extensions	
Basic Constraints	Subject Type= EndEntity
	Path Length Constraint=None
Key Usage	Digital Signature Key Encipherment Non-Repudiation Data Encipherment Key Agreement
Enhanced key usage (property)	Client Authentication
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-client-issuing [2] Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= https://www.trustfactory.net/repository/tf-online-client.crt
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.50318.2.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.trustfactory.net/repository [2] Policy Identifier=1.3.6.1.4.1.50318.3.1
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.trustfactory.net/crl/tf-client-subscriber.crl
SubjectAltName	*emailAddress*
Properties	
Thumbprint algorithm	SHA1

10.4 PERSONALPASS PREMIUM CERT PROFILE

PERSONALPASS PREMIUM	V1 Fields
Version	V3
Serial number	
Signature algorithm	sha256RSA
Signature hash algorithm	sha256

Issuer	CN = TrustFactory Client Issuing Certificate Authority
	OU = TrustFactory PKI Operations
	O = TrustFactory(Pty)Ltd
	L = Johannesburg
	S = Gauteng
	C = ZA

Validity	*1, 2 or 3 years*

Subject	CN = *first name and surname*
	OU = *(optional)*
	O = *(optional)*
	L = *(optional)*
	ST = *(optional)*
	C = *country*
	emailAddress=

Public key	RSA (*minimum 2048 bits*)
Extensions	
Basic Constraints	Subject Type= EndEntity
	Path Length Constraint=None
Key Usage	Digital Signature Key Encipherment Non-Repudiation Data Encipherment Key Agreement
Enhanced key usage (property)	Client Authentication
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-client-issuing [2] Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= https://www.trustfactory.net/repository/tf-online-client.crt
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.50318.2.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.trustfactory.net/repository [2] Policy Identifier=1.3.6.1.4.1.50318.3.1 [3] Policy Identifier=1.3.6.1.4.1.50318.3.2
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.trustfactory.net/crl/tf-client-subscriber.crl
SubjectAltName	*emailAddress*
Properties	
Thumbprint algorithm	SHA1