PUBLIC

TrustFactory Client Issuing CA Certification Practice Statement

31st March 2020
Version: 1.7

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

1.0 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

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

1.3 PKI Participants

1.3.1 TrustFactory 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 will be responsible for:

- Accepting, evaluating, approving or rejecting the registration of Certificate applications;
- Registering Subscribers for certification services;
- Providing systems to facilitate the identification of Subscribers (according to the type of Certificate requested);
- Using authorized documents or sources of information to evaluate and authenticate an Applicant;
- 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 will 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 have 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 will identify 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:

- **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.

- **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.

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

1.5.2 Contact Person

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

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 www.trustfactory.net. This opens an email client that sends an email to abuse@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

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

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

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

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

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Legal Entity is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.

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

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

Attestation Letter: A letter attesting that Subject Identity Information is correct.

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

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

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

Certificate Beneficiaries: The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate, all Application Software Suppliers with whom TrustFactory Client Issuing CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier, and all Relying Parties who reasonably rely on a Valid Certificate.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Individual: A natural person.

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: An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate. See also OCSP Responder.

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

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

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

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

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

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

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2 (Identity/ Qualifications of Assessor).

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

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

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.

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

AATL	Adobe Approved Trust List
AES	Advanced Electronic Signature
AICPA	American Institute of Certified Public Accountants

API	Application Programming Interface
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
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
EKU	Extended Key Usage
ERA	Enterprise Registration Authority
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ID	Identity document
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PKI	Public Key Infrastructure
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority
RFC	Request for Comments
SAAA	South African Accreditation Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VAT	Value Added Tax

2.0 Publication and Repository Responsibilities

2.1 Repositories

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

2.3 Time or Frequency of Publication

The TrustFactory PA will annually review 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 will increment the version number and add 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.

3.0 Identification and Authentication

TrustFactory Client Issuing CA will rely 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 will be the name associated with the Subscriber to which the Subscriber Certificate is to be issued.

3.1.2 Need for Names to be Meaningful

The value of the common name attribute used in naming Subscribers 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) will not be permitted, except for the purposes of issuing certificates for testing or demonstration purposes.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished names in Certificates are interpreted using X.500 standards and ASN.1 syntax. 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 include an organization identity, Applicants are required to provide the organization's name and registered or trading address. For all Certificates, the legal existence, legal name, assumed name, legal form (where included in the request or part of the legal name in the jurisdiction of incorporation) and requested address of the organization are verified using one of the following:

- A government agency in the jurisdiction of the Applicant, or a superior governing governmental agency if the Applicant claims they are a government agency themselves; 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;
- An independent verification agency that operates in the jurisdiction in which the company is registered; or
- A site visit by the RA

3.2.2.2 Use of Tradename or DBA name

For organization 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.

3.2.3 Authentication of Individual identity

TrustFactory RAs will authenticate individuals depending upon the type of Certificate as indicated below.

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 will confirm the authenticity of the individual by means of face to face meeting with the subscriber, or on a procedure that provides an equivalent assurance. 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

- The individual name, that is the Subject of the certificate, must present at a face-to-face meeting with the RA or authorized RA representative and submit a hand-signed subscriber agreement.
- The Applicant is required to submit 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 will confirm the authenticity of the individual by means of face to face meeting with the subscriber, or on a procedure that provides an equivalent assurance. 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.

3.2.4 Non Verified Subscriber Information

TrustFactory does not verify the Subject Organizational Unit (OU) field in a Certificate. For all other fields, information that is not verified will not be included in the certificates.

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 will verify the Authority Letter and thereafter TrustFactory will 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.

3.3.3 Identification and Authentication for Renewal Requests

Certificate renewal requests will be 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 and the Subscriber submits a CSR containing the existng Public Key.

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

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

If at any point any Subject name information embodied in a Certificate is changed in any way, then the new certificate registration process will be followed and the identity proofing procedures for a new certificate outlined in this requirement will be re-performed and a new Certificate issued with the validated information.

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

3.4 Identification and Authentication for Revocation Request

TrustFactory will accept revocation requests from:

1. The Subscriber, requested via the Subscriber Management Portal (login to the portal is acceptable authentication of the subscriber)
2. The RA Administrator, requested via the RA application API or pre-determined trusted path
3. The TrustFactory operations team, after it is approved by the CA Administrator
4. 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.

4.0 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

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

- the Applicant directly via the TrustFactory website at www.trustfactory.net
- an approved RA, provided that it is authorized by the original Applicant, or
- an organization administrator (Applicant Representative) who retains responsibility for the Private Key on behalf of an organization

The Subscriber Management Portal on the TrustFactory website is the mechanism through which an Applicant / Subscriber submits new certificate requests as well as renewal requests, re-key and revocation requests.

Approved external RAs can submit certificate application via a trusted path and the RA 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 will not accept Certificate applications. The blacklist includes all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns.

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 will 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 request; 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 will validate 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 will be 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 will 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, provided that the data or document was obtained no more than 825 days prior to issuing the Certificate.

TrustFactory Client Issuing CA checks for High Risk Certificate Requests and will 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 will 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 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 will endeavor 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. TrustFactory Client Issuing CAs will communicate with approved RAs through a pre-established trusted path (generally this is over a secure API). TrustFactory Client Issuing CA will 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 enrollment 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 over the software API, if they were involved in the initial enrollment.

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

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 original Certificate will be revoked after renewed certificate is issued.

The TrustFactory system will automatically generate 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 will be sent the registered subscriber email address.

4.6.2 Who May Request Renewal

TrustFactory Client Issuing CA may accept a renewal request from the Subscriber or an RA, 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 login to the Subscriber Management Portal or the RA's management system.

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 same procedures as the initial registration if 825 days has elapsed since the previous validation.

TrustFactory will 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 will be 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, 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 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 is acceptable. A CSR is required for issuing the new certificate.

TrustFactory will reuse 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 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 remain the same; and
- Only subject detail email address field modifications are submitted in the modification request.

The original Certificate will be 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 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. A Certificate signing request is mandatory with any new Public Key to be certified. A modification/re-issue is requested only via the Subscriber Management Portal

4.8.3 Processing Certificate Modification Requests

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

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

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 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; or

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/SSLkeys), 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 subscribers 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)

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

- 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;
- Overdue payment of applicable fees by the Subscriber;
- Under certain licensing arrangements, TrustFactory Client Issuing CA may revoke Certificates following expiration or termination of the license agreement;
- 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.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

Not applicable.

4.9.2 Who Can Request Revocation

TrustFactory Client Issuing CA will accept revocation requests submitted via login to the Subscriber Management Portal. A revocation request may be accepted from an organization administrator 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 www.trustfactory.net. This opens an email client that sends an email to abuse@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.

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

Once revoked, the serial number of the Certificate and the date and time will be 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 www.trustfactory.net. This opens an email client that sends an email to abuse@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 SSL Issuing CA shall notify the Subscriber of the revocation of a Certificate using the email address submitted during the enrollment 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

5.0 Facility, Management, and Operational Controls

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

5.1 Physical Controls

Controls are as defined in the TrustFactory CP.

5.1.1 Site Location and Construction

Controls are as defined in the TrustFactory CP.

5.1.2 Physical Access

Controls are as defined in the TrustFactory CP.

5.1.3 Power and Air Conditioning

Controls are as defined in the TrustFactory CP.

5.1.4 Water Exposures

Controls are as defined in the TrustFactory CP.

5.1.5 Fire Prevention and Protection

Controls are as defined in the TrustFactory CP.

5.1.6 Media Storage

Controls are as defined in the TrustFactory CP.

5.1.7 Waste Disposal

Controls are as defined in the TrustFactory CP.

5.1.8 Off-Site Backup

Controls are as defined in the TrustFactory CP.

5.2 Procedural Controls

Controls are as defined in the TrustFactory CP.

5.2.1 Trusted Roles

Controls are as defined in the TrustFactory CP

5.2.2 Number of Persons Required per Task

Controls are as defined in the TrustFactory CP

5.2.3 Identification and Authentication for Each Role

Controls are as defined in the TrustFactory CP.

5.2.4 Roles Requiring Separation of Duties

Controls are as defined in the TrustFactory CP

5.3 Personnel Controls

Controls are as defined in the TrustFactory CP.

5.3.1 Qualifications, Experience, and Clearance Requirements

Controls are as defined in the TrustFactory CP.

5.3.2 Background Check Procedures

Controls are as defined in the TrustFactory CP.

5.3.3 Training Requirements

Controls are as defined in the TrustFactory CP.

5.3.4 Retraining Frequency and Requirements

Controls are as defined in the TrustFactory CP.

5.3.5 Job Rotation Frequency and Sequence

Controls are as defined in the TrustFactory CP.

5.3.6 Sanctions for Unauthorized Actions

Controls are as defined in the TrustFactory CP.

5.3.7 Independent Contractor Requirements

Controls are as defined in the TrustFactory CP.

5.3.8 Documentation Supplied to Personnel

Controls are as defined in the TrustFactory CP.

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 are automatically generated. Where this is not possible, a logbook, ceremony script, paper form, or other physical mechanism will be used. All security audit logs, both electronic and non-electronic, will be retained and made available during compliance audits.

TrustFactory Client Issuing CA ensures all events relating to the lifecycle of Certificates are logged in a manner to ensure the traceability to a person in a trusted role for any action required for CA services.

The TrustFactory Client Issuing CA, and RA's where applicable, 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, RA and Subscriber Certificate lifecycle management events, including:
   a. Certificate requests, renewal, and re-key requests, and revocation;
   b. All verification activities stipulated in this CPS;
   c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
   d. Name of submitting RA,
   e. Acceptance and rejection of certificate requests;
   f. Issuance of Certificates;
   g. The subscriber's acceptance of the Subscriber Agreement; and
   h. Where required under privacy legislation, the Subscriber's consent to allow TrustFactory to keep records containing personal data, pass this information to specified third parties, and publication of certificates.
   i. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
   a. Successful and unsuccessful PKI system access attempts;
   b. PKI and security system actions performed;
   c. Security profile changes;
   d. System crashes, hardware failures, and other anomalies; (MANUAL)
   e. Firewall and router activities; and
   f. Entries to and exits from the CA facility.

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

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

5.4.2 Frequency of Processing Logs

Audit logs are reviewed as follows:

1. the Security Officer reviews logs of security events on the IT and 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 quarterly audits.

Unauthorized or suspicious activity detected during the reviews is investigated.

Any important operation involving the Issuing CA HSM is conducted through documented CA ceremony scripts which are witnessed by the internal auditors.

5.4.3 Retention Period for Audit Log

Controls are as defined in the TrustFactory CP

5.4.4 Protection of Audit Log

Controls are as defined in the TrustFactory CP

5.4.5 Audit Log Backup Procedures

Audit logs are backed-up using online backup mechanism to the disaster recovery site, and atleast 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)

Controls are as defined in the TrustFactory CP

5.4.7 Notification to Event-Causing Subject

No requirements specified.

5.4.8 Vulnerability Assessments

1. Controls are as defined in the TrustFactory CP

5.5 Records Archival

5.5.1 Types of Records Archived

All records related to auditable events defined in Section 5.4.1 should be archived.

5.5.2 Retention Period for Archive

Controls are as defined in the TrustFactory CP

5.5.3 Protection of Archive

Controls are as defined in the TrustFactory CP

5.5.4 Archive Backup Procedures

Controls are as defined in the TrustFactory CP

5.5.5 Requirements for Timestamping of Records

Controls are as defined in the TrustFactory CP

5.5.6 Archive Collection System (Internal or External)

Controls are as defined in the TrustFactory CP

5.5.7 Procedures to Obtain and Verify Archive Information

Controls are as defined in the TrustFactory CP

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Controls are as defined in the TrustFactory CP

5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

Controls are as defined in the TrustFactory CP

5.7.3 Recovery Procedures After Key Compromise

Controls are as defined in the TrustFactory CP

5.7.4 Business Continuity Capabilities after a Disaster

Controls are as defined in the TrustFactory CP

5.8 CA or RA Termination

Controls are as defined in the TrustFactory CP.

6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The signing key pair for the TrustFactory Client Issuing CA was created during the initial startup of the CA application and 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 GenerationTrustFactory Client Issuing CA does not provide subscriber key generation or key management services

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

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

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

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

Controls as per the TrustFactory CP

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

Controls as per the TrustFactory CP

6.2.3 Private Key Escrow

Controls as per the TrustFactory CP

6.2.4 Private Key Backup

Controls as per the TrustFactory CP

6.2.5 Private Key Archival

Controls as per the TrustFactory CP

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Controls as per the TrustFactory CP

6.2.7 Private Key Storage on Cryptographic Module

Controls as per the TrustFactory CP

6.2.8 Method of Activating Private Key

Controls as per the TrustFactory CP

6.2.9 Method of Deactivating Private Key

Controls as per the TrustFactory CP

6.2.10 Method of Destroying Private Key

Controls as per the TrustFactory CP

6.2.11 Cryptographic Module Capabilities

See Section 6.2.1

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 2 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

Activation data used to activate TrustFactory Client Issuing CA Private Keys are generated during a key ceremony (Refer to Section 6.1.1). Activation data is generated automatically by the HSM and stored on smartcards under shareholder and security officer control and handed to the shareholder, who is a trusted person.

6.4.2 Activation Data Protection

TrustFactory Client Issuing CA activation data is protected from disclosure through storing on smart cards and locking away at a secure location inside tamper-evident sealed packaging.

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

Controls as per the TrustFactory CP.

6.5.1 Specific Computer Security Technical Requirements

Controls as per the TrustFactory CP.

6.5.2 Computer Security Rating

Controls as per the TrustFactory CP.

6.6 Lifecycle Technical Controls

Controls as per the TrustFactory CP.

6.6.1 System Development Controls

Controls as per the TrustFactory CP

6.6.2 Security Management Controls

Controls as per the TrustFactory CP.

6.6.3 Lifecycle Security Controls

Controls as per the TrustFactory CP.

6.7 Network Security Controls

Controls as per the TrustFactory CP.

6.8 Time Stamping

Controls as per the TrustFactory CP.

7.0 Certificate, CRL, and OCSP Profiles

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

7.1 Certificate Profile

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.

7.1.1 Version Number(s)

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

7.1.2 Certificate 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.

Subscriber Certificates

a. certificatePolicies
This extension is not set as critical.
certificatePolicies:policyIdentifier is populated in accordance to Section 1.2

b. cRLDistributionPoints
This extension is not set as critical, and it contains the HTTP URL of the CA's CRL service.

c. authorityInformationAccess
This extension is not set as critical, and it contains the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

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

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

7.1.3 Algorithm Object Identifiers

TrustFactory uses the SHA-2 hash algorithm across all its certificates.

7.1.4 Name Forms

7.1.4.1. Issuer Information

TrustFactory Client Issuing CA issues Certificates with name forms compliant to RFC 5280.

Name chaining of a Certificate is performed by matching the content of the Certificate Issuer Distinguished Name field of the Certificate to the Subject Distinguished Name of the Issuing CA that issued the Certificate.

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

8.0 Compliance Audit and Other Assessments

TrustFactory Client Issuing CA is audited for compliance to one of the current applicable version of one or more of the following standards:

- WebTrust for Certification Authorities
- South African Accreditation Authority – ECT Act Regulations

8.1 Frequency and Circumstances of Assessment

Controls as per TrustFactory CP.

8.2 Identity/Qualifications of Assessor

Controls as per TrustFactory CP

8.3 Assessor's Relationship to Assessed Entity

Controls as per TrustFactory CP.

8.4 Topics Covered by Assessment

Controls as per TrustFactory CP.

8.5 Actions Taken as a Result of Deficiency

Controls as per TrustFactory CP.

8.6 Communications of Results

Controls as per TrustFactory CP.

9.0 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Controls as per the TrustFactory CP

9.1.2 Certificate Access Fees

Controls as per the TrustFactory CP

9.1.3 Revocation or Status Information Access Fees

Controls as per the TrustFactory CP

9.1.4 Fees for Other Services

Controls as per the TrustFactory CP

9.1.5 Refund Policy

Controls as per the TrustFactory CP

9.2 Financial Responsibility

Controls as per the TrustFactory CP

9.2.1 Insurance Coverage

Controls as per the TrustFactory CP

9.2.2 Other Assets

Controls as per the TrustFactory CP

9.2.3 Insurance or Warranty Coverage for End Entities

Controls as per the TrustFactory CP

9.3 Confidentiality of Business Information

Controls as per the TrustFactory CP.

9.3.1 Scope of Confidential Information

Controls as per the TrustFactory CP

9.3.2 Information Not Within the Scope of Confidential Information

Controls as per the TrustFactory CP

9.3.3 Responsibility to Protect Confidential Information

Controls as per the TrustFactory CP.

9.4 Privacy of Personal Information

Controls as per the TrustFactory CP.

9.4.1 Privacy Plan

Controls as per the TrustFactory CP.

9.4.2 Information Treated as Private

Controls as per the TrustFactory CP.

9.4.3 Information Not Deemed Private

Controls as per the TrustFactory CP.

9.4.4 Responsibility to Protect Private Information

Controls as per the TrustFactory CP.

9.4.5 Notice and Consent to Use Private Information

Controls as per the TrustFactory CP.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Controls as per the TrustFactory CP.

9.4.7 Other Information Disclosure Circumstances

Controls as per the TrustFactory CP.

9.5 Intellectual Property rights

Controls as per the TrustFactory CP.

9.6 Representations and Warranties

Controls as per the TrustFactory CP.

9.6.1 CA Representations and Warranties

Controls as per the TrustFactory CP

9.6.2 RA Representations and Warranties

Controls as per the TrustFactory CP

9.6.3 Subscriber Representations and Warranties

Controls as per the TrustFactory CP

-

9.6.4 Relying Party Representations and Warranties

Controls as per the TrustFactory CP.

9.6.5 Representations and Warranties of Other Participants

Controls as per the TrustFactory CP.

9.7 Disclaimers of Warranties

Controls as per the TrustFactory CP.

9.8 Limitations of Liability

Controls as per the TrustFactory CP.

9.9 Indemnities

Controls as per the TrustFactory CP.

9.10 Term and Termination

Controls as per the TrustFactory CP.

9.10.1 Term

Controls as per the TrustFactory CP.

9.10.2 Termination

Controls as per the TrustFactory CP.

9.10.3 Effect of Termination and Survival

Controls as per the TrustFactory CP.

9.11 Individual Notices and Communications with Participants

Controls as per the TrustFactory CP.

9.12 Amendments

Controls as per the TrustFactory CP

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

Controls as per the TrustFactory CP.

9.12.2 Notification Mechanism and Period

Controls as per the TrustFactory CP.

9.12.3 Circumstances Under Which OID Must be Changed

Controls as per the TrustFactory CP.

9.13 Dispute Resolution Provisions

Controls as per the TrustFactory CP.

9.14 Governing Law

Controls as per the TrustFactory CP.

9.15 Compliance with Applicable Law

Controls as per the TrustFactory CP.

9.16 Miscellaneous Provisions

Controls as per the TrustFactory CP.

9.16.1 Entire Agreement

Controls as per the TrustFactory CP.

9.16.2 Assignment

Controls as per the TrustFactory CP.

9.16.3 Severability

Controls as per the TrustFactory CP.

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

Controls as per the TrustFactory CP

9.17 Other Provisions

Controls as per the TrustFactory CP

Annexure A: Client CA Certificate Profiles

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

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 or 2 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)	Email Protection
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

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 or 2 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)	Email Protection 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

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 or 2 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)	Email Protection 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