PUBLIC

TrustFactory Certification Authority Certificate Policy

Date: 05 November 2024
Version 1.11

Shital Naik

Digitally signed by Shital Naik
Date: 2024.11.05 12:41:32 +02'00'

Table of Contents

1 Introduction 9

1.1 Overview 9

1.2 Document Name and Identification 10
1.2.1 Document Revisions 10

1.3 PKI participants 11
1.3.1 Certification Authorities 11
1.3.2 Registration Authorities 11
1.3.3 Subscribers 11
1.3.4 Relying Parties 12
1.3.5 Other Participants 12

1.4 Certificate usage 12
1.4.1 Appropriate Certificate Usage 12
1.4.2 Prohibited Certificate Usage 12

1.5 Policy Administration 12
1.5.1 Organization Administering the Document 12
1.5.2 Contact Person 13
1.5.3 Person Determining CPS Suitability for the Policy 13
1.5.4 CP Approval Procedures 13

1.6 Definitions and acronyms 13
1.6.1 Definitions 13
1.6.2 Acronyms 18

2 Publication and Repository Responsibilities 20

2.1 Repositories 20

2.2 Publication of Certificate Information 20
2.2.1 Name of Policy/Guideline/Requirement Standard 20

2.3 Time or Frequency of Publication 20

2.4 Access controls on repositories 21

3 Identification and Authentication 22

3.1 Naming 22
3.1.1 Types of Names 22
3.1.2 Need for Names to be Meaningful 22
3.1.3 Anonymity or Pseudonymity of Subscribers 22
3.1.4 Rules for Interpreting Various Name Forms 22
3.1.5 Uniqueness of Names 22
3.1.6 Recognition, Authentication, and Role of Trademarks 22

3.2 Initial Identity Validation 22
3.2.1 Method to Prove Possession of Private Key 23
3.2.2 Authentication of Organization Identity and Domain Identity 23
3.2.3 Authentication of Individual identity 23
3.2.4 Non Verified Subscriber Information 23
3.2.5 Validation of Authority 23
3.2.6 Criteria for Interoperation 23

3.3 Identification and Authentication for Re-key Requests 23
3.3.1 Identification and Authentication for Routine Re-key 24
3.3.2 Identification and Authentication for Re-key after Revocation 24

3.4 Identification and Authentication for Revocation Request 24

4 Certificate Lifecycle Operational Requirements 25

4.1 Certificate Application 25

4.1.1 Who Can Submit a Certificate Application 25
4.1.2 Enrollment Process and Responsibilities 25

4.2 Certificate Application Processing 25
4.2.1 Performing Identification and Authentication Functions 25
4.2.2 Approval or Rejection of Certificate Applications 26
4.2.3 Time to Process Certificate Applications 26

4.3 Certificate Issuance 26
4.3.1 CA Actions during Certificate Issuance 26
4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate 26

4.4 Certificate Acceptance 26
4.4.1 Conduct Constituting Certificate Acceptance 26
4.4.2 Publication of the Certificate by the CA 26
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 27

4.5 Key Pair and Certificate Usage 27
4.5.1 Subscriber Private Key and Certificate Usage 27
4.5.2 Relying Party Public Key and Certificate Usage 27

4.6 Certificate Renewal 27
4.6.1 Circumstances for Certificate Renewal 27
4.6.2 Who May Request Renewal 27
4.6.3 Processing Certificate Renewal Requests 28
4.6.4 Notification of New Certificate Issuance to Subscriber 28
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 28
4.6.6 Publication of the Renewal Certificate by the CA 28
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 28

4.7 Certificate Re-Key 28
4.7.1 Circumstances for Certificate Re-Key 28
4.7.2 Who May Request Certification of a New Public Key 28
4.7.3 Processing Certificate Re-Key Requests 29
4.7.4 Notification of New Certificate Issuance to Subscriber 29
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 29
4.7.6 Certificate Publication of the Re-Keyed Certificate by the CA 29
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 29

4.8 Certificate Modification 29
4.8.1 Circumstances for Certificate Modification 29
4.8.2 Who May Request Certificate Modification 29
4.8.3 Processing Certificate Modification Requests 29
4.8.4 Conduct Constituting Acceptance of a Modified Certificate 29
4.8.5 Certificate Publication of the Modified Certificate by the CA 29
4.8.6 Notification of Certificate Issuance by the CA to Other Entities 30

4.9 Certificate Revocation and Suspension 30
4.9.1 Circumstances for Revocation 30
4.9.2 Who Can Request Revocation 30
4.9.3 Procedure for Revocation Request 30
4.9.4 Revocation Request Grace Period 30
4.9.5 Time Within Which CA Must Process the Revocation Request 30
4.9.6 Revocation Checking Requirements for Relying Parties 31
4.9.7 CRL Issuance Frequency 31
4.9.8 Maximum Latency for CRLs 31
4.9.9 On-Line Revocation/Status Checking Availability 31
4.9.10 On-Line Revocation Checking Requirements 31
4.9.11 Other Forms of Revocation Advertisements Available 32
4.9.12 Special Requirements Related to Key Compromise 32
4.9.13 Circumstances for Suspension 32
4.9.14 Who Can Request Suspension 32
4.9.15 Procedure for Suspension Request 32
4.9.16 Limits on Suspension Period 32

4.10 Certificate Status Services 32
4.10.1 Operational Characteristics 32
4.10.2 Service Availability 32
4.10.3 Operational Features 32

4.11 End of Subscription 33

4.12 Key Escrow and Recovery 33
4.12.1 Key Escrow and Recovery Policy and Practices 33
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 33

5 Facility, Management, and Operational Controls 34

5.1 Physical Controls 34
5.1.1 Site Location and Construction 34
5.1.2 Physical Access 34
5.1.3 Power and Air Conditioning 34
5.1.4 Water Exposures 34
5.1.5 Fire Prevention and Protection 34
5.1.6 Media Storage 34
5.1.7 Waste Disposal 35
5.1.8 Off-Site Backup 35

5.2 Procedural Controls 35
5.2.1 Trusted Roles 35
5.2.2 Number of Persons Required per Task 36
5.2.3 Identification and Authentication for Each Role 36
5.2.4 Roles Requiring Separation of Duties 36

5.3 Personnel Controls 37
5.3.1 Qualifications, Experience, and Clearance Requirements 37
5.3.2 Background Check Procedures 37
5.3.3 Training Requirements 37
5.3.4 Retraining Frequency and Requirements 37
5.3.5 Job Rotation Frequency and Sequence 37
5.3.6 Sanctions for Unauthorized Actions 37
5.3.7 Independent Contractor Requirements 38
5.3.8 Documentation Supplied to Personnel 38

5.4 Audit Logging Procedures 38
5.4.1 Types of Events Recorded 38
5.4.2 Frequency of Processing Log 38
5.4.3 Retention Period for Audit Log 38
5.4.4 Protection of Audit Log 38
5.4.5 Audit Log Backup Procedures 38
5.4.6 Audit Collection System (Internal vs. External) 39
5.4.7 Notification to Event-Causing Subject 39
5.4.8 Vulnerability Assessments 39

5.5 Records Archival 39
5.5.1 Types of Records Archived 39
5.5.2 Retention Period for Archive 39
5.5.3 Protection of Archive 39
5.5.4 Archive Backup Procedures 39
5.5.5 Requirements for Time-Stamping of Records 39
5.5.6 Archive Collection System (Internal or External) 40
5.5.7 Procedures to Obtain and Verify Archive Information 40

5.6 Key Changeover 40

5.7 Compromise and Disaster Recovery 40
5.7.1 Incident and Compromise Handling Procedures 40
5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted 40
5.7.3 Recovery Procedures After Key Compromise 40
5.7.4 Business Continuity Capabilities after a Disaster 40

5.8 CA or RA Termination 40

6 Technical Security Controls 41

6.1 Key Pair Generation and Installation 41
6.1.1 Key Pair Generation 41
6.1.2 Private Key Delivery to Subscriber 41
6.1.3 Public Key Delivery to Certificate Issuer 41
6.1.4 CA Public Key Delivery to Relying Parties 41
6.1.5 Key Sizes 42
6.1.6 Public Key Parameters Generation and Quality Checking 42
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 42

6.2 Private Key Protection and Cryptographic Module Engineering Controls 42
6.2.1 Cryptographic Module Standards and Controls 42
6.2.2 Private Key (m of n) Multi-Person Control 43
6.2.3 Private Key Escrow 43
6.2.4 Private Key Backup 43
6.2.5 Private Key Archival 43
6.2.6 Private Key Transfer Into or From a Cryptographic Module 43
6.2.7 Private Key Storage on Cryptographic Module 43
6.2.8 Method of Activating Private Key 43
6.2.9 Method of Deactivating Private Key 44
6.2.10 Method of Destroying Private Key 44
6.2.11 Cryptographic Module Rating 44

6.3 Other Aspects of Key Pair Management 44
6.3.1 Public Key Archival 44
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 44

6.4 Activation Data 44
6.4.1 Activation Data Generation and Installation 44
6.4.2 Activation Data Protection 44
6.4.3 Other Aspects of Activation Data 45

6.5 Computer Security Controls 45
6.5.1 Specific Computer Security Technical Requirements 45
6.5.2 Computer Security Rating 45

6.6 Lifecycle Technical Controls 45
6.6.1 System Development Controls 45
6.6.2 Security Management Controls 45
6.6.3 Lifecycle Security Controls 45

6.7 Network Security Controls 45

6.8 Timestamping 45

7 Certificate, CRL, and OCSP Profiles 46

7.1 Certificate Profile 46
7.1.1 Version Number(s) 46
7.1.2 Certificate Content and Extensions 46
7.1.3 Algorithm Object Identifiers 46
7.1.4 Name Forms 49
7.1.5 Name Constraints 51
7.1.6 Certificate Policy Object Identifier 51
7.1.7 Usage of Policy Constraints Extension 51
7.1.8 Policy Qualifiers Syntax and Semantics 51
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 51

7.2 CRL Profile 51
7.2.1 Version Number(s) 51
7.2.2 CRL and CRL Entry Extensions 51

7.3 OCSP Profile 51
7.3.1 Version Number(s) 52
7.3.2 OCSP Extensions 52

8 Compliance Audit and Other Assessments 53

8.1 Frequency and Circumstances of Assessment 53

8.2 Identity/Qualifications of Assessor 53

8.3 Assessor's Relationship to Assessed Entity 53

8.4 Topics Covered by Assessment 53

8.5 Actions Taken as a Result of Deficiency 54

8.6 Communications of Results 54

8.7 Self-Audits 54

9 Other Business and Legal Matters 55

9.1 Fees 55
9.1.1 Certificate Issuance or Renewal Fees 55
9.1.2 Certificate Access Fees 55
9.1.3 Revocation or Status Information Access Fees 55
9.1.4 Fees for Other Services 55
9.1.5 Refund Policy 55

9.2 Financial Responsibility 55
9.2.1 Insurance Coverage 55
9.2.2 Other Assets 55
9.2.3 Insurance or Warranty Coverage for End Entities 55

9.3 Confidentiality of Business Information 55
9.3.1 Scope of Confidential Information 55
9.3.2 Information Not Within the Scope of Confidential Information 55
9.3.3 Responsibility to Protect Confidential Information 56

9.4 Privacy of Personal Information 56
9.4.1 Privacy Plan 56
9.4.2 Information Treated as Private 56
9.4.3 Information Not Deemed Private 56
9.4.4 Responsibility to Protect Private Information 56
9.4.5 Notice and Consent to Use Private Information 56
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 56
9.4.7 Other Information Disclosure Circumstances 56

9.5 Intellectual Property rights 56

9.6 Representations and Warranties 56
9.6.1 CA Representations and Warranties 56
9.6.2 RA Representations and Warranties 57
9.6.3 Subscriber Representations and Warranties 58
9.6.4 Relying Party Representations and Warranties 58
9.6.5 Representations and Warranties of Other Participants 59

9.7 Disclaimers of Warranties 59

9.8 Limitations of Liability 59

9.9 Indemnities 60
9.9.1 Indemnification by TrustFactory CA 60
9.9.2 Indemnification by Subscribers 60
9.9.3 Indemnification by Relying Parties 60

9.10 Term and Termination 60
9.10.1 Term 60
9.10.2 Termination 60
9.10.3 Effect of Termination and Survival 60

9.11 Individual Notices and Communications with Participants 60

9.12 Amendments 61
9.12.1 Procedure for Amendment 61
9.12.2 Notification Mechanism and Period 61
9.12.3 Circumstances Under Which OID Must be Changed 61

9.13 Dispute Resolution Provisions 61

9.14 Governing Law 62

9.15 Compliance with Applicable Law 62

9.16 Miscellaneous Provisions 62
9.16.1 Entire Agreement 62
9.16.2 Assignment 62
9.16.3 Severability 62
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 62
9.16.5 Force Majeure 62

9.17 Other Provisions 63
ANNEXURE A RFC 6844 ERRATA 5065 64
ANNEXURE B CAA CONTACT TAG 65
ANNEXURE C Issuance of Certificates for .onion Domain Names 66

References and Acknowledgements

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

1 Introduction

This Certificate Policy (CP) establishes the requirements, policies and standards that apply to the products and services within the TrustFactory PKI hierarchy. The latest version may be found on the TrustFactory Repository at https://www.trustfactory.net/repository.

This CP follows the content and structure guidance provided in Internet Engineering Task Force (IETF) RFC 3647, dated November 2003. Where certain sections or topics of the RFC 3647 do not apply or requirements not defined then the term 'No stipulation' is used.

Where applicable, TrustFactory CAs conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and the Baseline Requirements, the Baseline Requirements take precedence over this document.

TrustFactory Certification Authorities (CA) are governed by this CP together with a Certification Practice Statement (CPS) applicable to each CA.

This CP applies to all Certificates issued by TrustFactory including its Root Certificates and any chained Subordinate CAs. Requirements, 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 the CPS – except to aid readability). The specific technical and procedural practices that apply to a specific CA are documented in the applicable CA's CPS. Root Certificates are used to manage Certificate hierarchies through the creation of one or more Subordinate CAs that issue certificates to public end entities **(all Subordinate CAs issuing public Certificates in accordance with this CP will be referred to as Issuing CAs).**

1.1 Overview

The purpose of this CP is to present TrustFactory policies, standards, processes and procedures in managing the hierarchy of the TrustFactory PKI CAs (Root CAs and Issuing CAs) and the issued Certificates. This CP helps to demonstrate compliance with formal industry accepted accreditations such as the South African Accreditation Authority and WebTrust. The TrustFactory PKI hierarchy is shown in Figure 1 below:

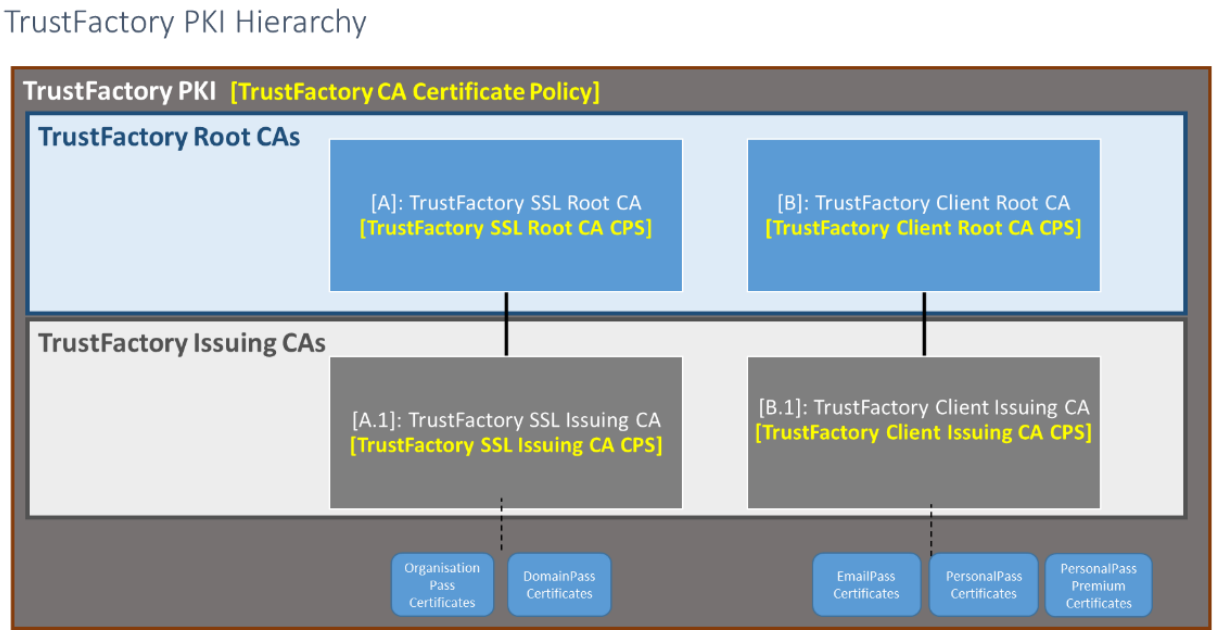

Figure 1: TrustFactory PKI Hierarchy

A CPS defines the *"procedures under which a Certificate is issued to a particular community and/or class of application with common security requirements"*. The CPS discloses how the TrustFactory Issuing CA meets the requirements of the CP and implements the controls through the certificate lifecycle management process.

Other documents that support or compliment the TrustFactory CP and CPSs include:

- The TrustFactory Warranty Policy that addresses issues on insurance
- The TrustFactory Privacy Policy on the protection of personal data
- The TrustFactory Subscriber Agreement
- The TrustFactory Relying Party Agreement

All applicable TrustFactory CP and CPSs are subject to audit by authorized auditors. Internal operational documents and the information security management system documents are confidential and not disclosed to the public. They are available to the authorized auditors.

The following TrustFactory CA Certificates subject names are governed by this CP:

1. CN= TrustFactory SSL Root Certificate Authority
2. CN= TrustFactory SSL Issuing Certificate Authority
3. CN= TrustFactory Client Root Certificate Authority
4. CN= TrustFactory Client Issuing Certificate Authority

TrustFactory expressly forbids the use of chaining services for MITM (Man in the Middle) SSL/TLS deep packet inspection.

1.2 Document Name and Identification

This document is the TrustFactory Certificate Policy.

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

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

1.3.6.1.4.1.50318.1	TrustFactory CA Certificate Policy
1.3.6.1.4.1.50318.2.1	TrustFactory SSL Root CA Certificates Practice Statement
1.3.6.1.4.1.50318.2.2	TrustFactory Client Root CA Certificates Practice Statement
1.3.6.1.4.1.50318.2.3	TrustFactory SSL Issuing CA Certificates Practice Statement
1.3.6.1.4.1.50318.2.4	TrustFactory Client Issuing CA Certificates Practice Statement

1.2.1 Document Revisions

Version	Description	Date
1.0	Initial for review	6 October 2017
1.1	Added certificate serial numbers. Error corrections.	7 December 2017
1.2	Updates to Section 9.1 Fees Other minor corrections	15 December 2017
1.3	Updated 6.1 to clarify that TrustFactory does not provide subscriber key management services. Updated notification of issuance: 4.3.2 and 4.4.3. Added renewal notification: 4.6.1 Updated Trusted Role definitions: 5.2.1 Added requirement for annual penetration testing: 5.4.8 Added Self Audits requirements: 8.7. Updated RA Warranties: 9.6.2 Updated 9.6.3 to clarify requirements for an Issuing CA as a Subscriber of a Root CA Updated Dispute Resolution Provisions: 9.13 Removed 3.2.2.1: Machine, Device, Department, and Role based Certificate Authentication Other updates based on CAB Forum Baseline Requirements changes Other minor corrections to improve clarity and remove duplications.	8 August 2018
1.4	Updates to 4.9.5 to incorporate latest CAB Forum changes on revocation requirements. Updates to 2.2 and 5.4.2 based on Audit recommendations. Other minor corrections.	21 November 2018

1.5	Updated 5.2.1 Trusted Roles responsibilities Updated 2.3 as per Mozilla requirement Updated 7.1.4 stated IP addresses not permitted Updated 4.9.2 to explain Certificate Problem reporting process Other minor corrections.	5 March 2019
1.6	Updated to incorporate details as required by Mozilla Root Store Policy. Aligned subsection heading to RFC3647 / CAB Forum Baseline Requirements Updated 6.1.1 for MS Root program requirement Updated 6.1.2 for MS Root program requirement Updated 8.1 for MS Root program requirement	31 March 2020
1.7	Updated to include subscriber information being sent over secure connection using APIs. Updated to include Trusted Agent and partners Updated and reworded certain sections: Section 2.2 Included latest CAB Baseline requirement and amended Section 4.2.1 Section 7.1.3.1 Section 7.1.3.2 Section 7.1.4	12 June 2021
1.8	Minor rewording added to sections relating to subscriber key generation 6.1 and 6.2	11 July 2022
1.9	Minor amendments to Sections 4.2.2. and 4.9.2	03 April 2023
1.10	Minor clarifications and amendments Sections 2.2 ; 9.8 ; 4.8.2 ; 4.8.3	14 August 2024
1.11	Minor changes to 6.3.2	31 October 2024

1.3 PKI participants

1.3.1 Certification Authorities

A Certification Authority (CA) is responsible for managing the certificate lifecycle management tasks related to: Subscriber registration, Certificate issuance, renewal, distribution and revocation. Certificate status information is provided through a Certificate Revocation List (CRL) distribution point and/or Online Certificate Status Protocol (OCSP) responder.

A Root CA creates its own self-signed certificate and also signs and issues Issuing CA Certificates.

An Issuing CA utilizes its Issuing CA Certificate to sign and issue Certificates to Subscribers, RAs or other end-entities.

1.3.2 Registration Authorities

A Registration Authority (RA) or Delegated Third Party is responsible for identifying and authenticating Applicants for Certificates, as well as providing requests for revocation, re-key, re-issuance and renewal of Certificates to the CA. TrustFactory and subordinate CAs may act as a Registration Authority for Certificates they issue. Domain Validations cannot be delegated to a third party and is only validated by the RA of the Issuer CA

Third party entities who are approved by the TrustFactory Policy Authority (PA) and who enter into an RA Agreement with TrustFactory may operate as an RA or Delegated Third Party. The RA must comply with all the requirements of this CP, and the CPS of the Issuing CA, and the terms of their RA Agreement. The RA must meet the qualification requirements of Section 5.3.1 and document retention requirements of Section 5.5.2. RAs may implement more stringent vetting practices based on their business needs.

1.3.3 Subscribers

Subscribers are both the end-entity that entered into a Subscriber Agreement with TrustFactory as well as the Subject of a Certificate. Subscribers can be either natural persons, legal entities or infrastructure components (such as servers, firewalls etc.) that have been issued with a Certificate by a TrustFactory Issuing CA.

Prior to verification and issuance of a Certificate, a Subscriber is referred to as an Applicant.

Issuing CAs/Subordinate CAs can also be referred to as subscribers of Root CAs.

1.3.4 Relying Parties

A Relying Party is an entity that relies on the validity of the binding of the Subscriber's Subject information to a public key in a Certificate. A Relying Party is responsible for checking the appropriate certificate status information (revocation information) and usage parameters to determine the suitability of the certificate for a particular use.

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 must identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.4 Certificate usage

1.4.1 Appropriate Certificate Usage

TrustFactory offers a range of distinct Certificate types, each having different usages for different applications. Certificate use is restricted by using Certificate extensions on key usage and extended key usage.

The relevant TrustFactory Issuing CA's CPS contains details about the different Certificate types and appropriate uses. Subscribers should ensure that the Certificate can be used for their intended application. Unauthorized use of Certificates may result in the voiding of warranties offered by TrustFactory to Subscribers and their Relying Parties.

1.4.2 Prohibited Certificate Usage

Any use of a TrustFactory Certificate that is not according to the defined key usage and extended key usage parameters or not consistent with applicable law is prohibited. Certificates are not authorized for use for any transactions above the payment or transaction limits specified in the TrustFactory Warranty Policy.

Certificates do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment into which the Certificate has been installed is free from defect, malware or virus.

Certificates issued under this CP 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

The TrustFactory Policy Authority (PA), is responsible for maintaining this Certificate Policy relating to all Certificates in the TrustFactory PKI hierarchy. The Policy Authority is the decision making body for all matters relating to the certificate lifecycle policy and management of the TrustFactory Root CAs, any subsequent Subordinate/Issuing CAs and approval of Registration Authorities (RA). The PA is composed of the TrustFactory General Manager and up to two members appointed by the Directors of the TrustFactory business.

TrustFactory accepts comments regarding this CP addressed to the Policy Authority at the address stated below.

1.5.1 Organization Administering the Document

TrustFactory Policy Authority, through the General Manager, administers the CP and CPS. Requests for information on the compliance of TrustFactory CAs with accreditation schemes as well as any other inquiry associated with this CP should be addressed to:

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

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

1.5.2 Contact Person

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

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

Subscribers, Relying Parties, Application Software Suppliers, and other third parties can report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, through the “Report Abuse” link on the TrustFactory website at 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 CP and the conformance of a CPS to this CP based on the results and recommendations received from a Qualified Auditor.

1.5.4 CP Approval Procedures

The TrustFactory Policy Authority reviews and approves any changes to the CP. Upon approval of a CP update by the Policy Authority, the new CP is published in the TrustFactory Repository at https://www.trustfactory.net/repository. The updated version is binding upon all current and new Subscribers and Relying Parties and supersedes previous versions of the CP.

Meaningful changes to this CP will be shown by a new version number and date, except where the amendments are purely clerical or improvements to document quality. The PA has the sole authority to decide if a version number change is required.

1.6 Definitions and acronyms

1.6.1 Definitions

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

Adobe Approved Trust List (AATL)	A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 9.0
Advanced Electronic Signature	A specific digital signature that complies with the requirements of the

(AES)	Electronic Communications and Transactions (ECT) Act of 2002 in the Republic of South Africa, and can be relied upon as evidence in a court of law.
Affiliate	A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Legal Entity is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.
Applicant Representative	A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.
Application Software Supplier	A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.
Attestation Letter	A letter attesting that Subject Identity Information is correct, written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
Business Entity	Any entity that is not a Private Organization, Government Entity, or non-commercial entity. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.
Certificate	An electronic document that uses a digital signature to bind a Public Key and an identity.
Certificate Beneficiaries	The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate, all Application Software Suppliers with whom TrustFactory CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier, and all Relying Parties who reasonably rely on a Valid Certificate.
Certificate Data	Certificate Requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.
Certificate Management Process	Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
Certificate Policy	A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
Certificate Problem Report	A complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Revocation List	A regularly updated timestamped list of revoked Certificates that is created

	and digitally signed by the CA that issued the Certificates.
Certification Authority (CA)	An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.
Certification Practice Statement (CPS)	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
Certificate Signing Request (CSR)	A message or data sent to a CA or RA to request the issuance of a certificate.
Compromise	A violation of a security policy that results in loss of control over sensitive information.
Country	Either a member of the United Nations or a geographic region recognized as a sovereign nation by at least two UN member nations.
Cross Certificate	A Certificate that is used to establish a trust relationship between two Root CAs.
Digital Signature	To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made.
Domain Name	The label assigned to a node in the Domain Name System.
Domain Name System (DNS)	An Internet service that translates Domain Names into IP addresses.
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
Domain Name Registrant	Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
ECT Act	The Electronic Communications and Transactions (ECT) Act of the Government of South Africa**.**
Enterprise RA	An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization or its subsidiaries. An Enterprise RA may also authorize issuance of client authentication Certificates to partners, customers, or affiliates wishing to interact with that organization.
Expiry Date	The "Not After" date in a Certificate that defines the end of a Certificate's Validity Period.
Fully-Qualified Domain Name (FQDN)	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
Government Entity	A government-operated legal entity, agency, department, ministry, branch,

	or similar element of the government of a Country, or political subdivision within such Country (such as a state, province, city, county etc.).
Hash	An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that: ▪ A message yields the same result every time the algorithm is executed using the same message as input. ▪ It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm. ▪ It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.
Hardware Security Module (HSM)	A HSM is type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.
Internal Server Name	A server name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.
Incorporate by Reference	To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.
Incorporating Agency	In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.
Individual	A natural person.
Issuing CA	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Jurisdiction of Incorporation	In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.
Key Compromise	A Private Key is said to be Compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it.
Key Pair	The Private Key and its associated Public Key.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a Country's legal system.
Object Identifier (OID)	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
OCSP Responder	An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
Online Certificate Status Protocol (OCSP)	An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate. See also OCSP Responder.

Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Private Organization	A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Public Key Infrastructure (PKI)	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key cryptography.
Publicly-Trusted Certificate	A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 8.2 (Identity/ Qualifications of Assessor).
Qualified Government Information Source	A database maintained by a Government Entity.
Qualified Government Tax Information Source	A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals.
Qualified Independent Information Source	A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar.
Registration Authority (RA)	Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the Certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
Relying Party	Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such supplier merely displays information relating to a Certificate.
Repository	An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response. (https://www.trustfactory.net/repository).
Root CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the commonName field.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber	A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued when the Applicant/Subscriber is an Affiliate of the CA.
Trusted Platform Module (TPM)	A hardware cryptographic device which is defined by the Trusted Computing Group. https://www.trustedcomputinggroup.org/specs/TPM.
Trustworthy System	Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name.
Validation Specialists	Someone who performs the information verification duties specified by these Requirements.
Validity Period	The period of time measured from the date when the Certificate is issued until the Expiry Date.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Vetting Agent	Someone who performs the information verification duties specified by these Requirements.
WebTrust Program for CAs	The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities.
WebTrust Seal of Assurance	An affirmation of compliance resulting from the WebTrust Program for CAs.
WHOIS	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.
Wildcard Certificate	A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.
X.509	The standard of the ITU-T (International Telecommunications Union-T) for Certificates.

1.6.2 Acronyms

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

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

2 Publication and Repository Responsibilities

2.1 Repositories

The legal repository for all TrustFactory CA public facing documentation is https://www.trustfactory.net/repository.

Published information may be updated from time to time as per Section 9.12.

TrustFactory CAs do 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 a TrustFactory CA.

2.2 Publication of Certificate Information

TrustFactory CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (excludes baseline requirements for the issuance and Management of Publicly-Trusted S/MIME Certificates) published at https://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

TrustFactory CA publishes this CP and any CPS, CA Certificates, Subscriber Agreements, Relying Party agreements, and CRLs in Repositories. This document specifies the policies and procedures that TrustFactory PKI adopts to meet the current versions of the following policies, guidelines and requirements:

2.2.1 Name of Policy/Guideline/Requirement Standard

The Certification Authority / Browser Forum (“CAB Forum”) Baseline Requirements for the Issuance and Management of Publicly – Trusted Certificates (“Baseline Requirements”) (excludes baseline requirements for the issuance and Management of Publicly-Trusted S/MIME Certificates)
The CAB Forum Network and Certificate System Security Requirements
Microsoft Trusted Root Store (Program Requirements)
The Adobe Approved TrustList Technical Requirements
Mozilla Root Store Policy
RFC 3647 of Internet Engineering Task Force (IETF) for Certificate policy and Certification Practice Statement

TrustFactory CA publishes the current status of issued certificates through CRLs in the Repository or an Online Certificate Status Protocol (OCSP) responder. TrustFactory does not maintain an X.500 or LDAP directory system for the subscriber certificates it issues.

CRLs should contain entries for all revoked unexpired Certificates. TrustFactory CAs may choose to maintain the serial numbers of expired Certificates on a CRL to further promote additional security.

TrustFactory SSL Issuing CAs shall host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA shall host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired.

2.3 Time or Frequency of Publication

TrustFactory CAs annually review and update the Certificate Policy and/or Certification Practice Statement to ensure they comply with the latest version of the Baseline Requirements, standards, laws and regulations or other circumstances. New or modified versions of this CP, the CPS, Subscriber Agreements, or Relying Party agreements are published within ten days after being approved and digitally signed by the Policy Authority.

In order to reference that the annual review of a Certificate Policy and/or Certification Practice Statement has taken place, TrustFactory shall 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

TrustFactory CAs provide public read only access to its Repositories. Security controls shall be implemented to prevent unauthorized persons from adding, deleting, or modifying repository entries. TrustFactory assures the integrity and authenticity of its public documentation by digitally signing the Adobe PDF format of the documents.

TrustFactory CA shall continue to be made publicly available all Audit, CP, CPS documents as required by Mozilla's CA Certificate Policy and the BRs

3 Identification and Authentication

TrustFactory CAs maintain documented practices and procedures to authenticate the identity and/or other attributes of the Applicant. TrustFactory CAs may also 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 Issuing CA.

The TrustFactory PA shall review and approve applications from entities seeking to become part of a TrustFactory CA's hierarchy, either as Subordinate CA to a Root CA or seeking chaining services or as an RA, Enterprise RA.

3.1 Naming

3.1.1 Types of Names

TrustFactory CAs follow the X.500 distinguished names rules to identify a Subscriber.

3.1.2 Need for Names to be Meaningful

TrustFactory CAs shall use distinguished names to identify the Subject of the end entity Certificates.

3.1.3 Anonymity or Pseudonymity of Subscribers

TrustFactory CAs shall not issue anonymous or pseudonymous certificates.

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

Each CA shall ensure that each of its subscribers is identifiable by a distinguished name. Each X.500 name assigned to a subscriber by a CA (i.e., in that CA's namespace) shall identify that subscriber. Name uniqueness is in general not enforced.

3.1.6 Recognition, Authentication, and Role of Trademarks

Applicants are prohibited from using names in their Certificate that infringe upon the intellectual property rights of others. TrustFactory Issuing CA does not verify whether an Applicant has intellectual property rights in the name appearing in the Certificate application or arbitrate, mediate or otherwise resolve any dispute concerning the ownership of any Domain Name, trademark, trade name or service mark. TrustFactory Issuing CA reserves the right, without liability to any Applicant, to reject an application because of such a dispute.

TrustFactory CAs may reject any applications or require revocation of any Certificate that is part of a dispute.

3.2 Initial Identity Validation

TrustFactory CAs/RAs shall validate or verify the Applicant using any legal means of communication or investigation necessary to identify the Legal Entity or individual.

TrustFactory RAs may delegate meetings with customers to trusted agents. The TrustFactory RA remains responsible for validation and verification of the legal entity or individual based on the information gathered by a trusted agent.

TrustFactory CAs may rely on and re-use the successfully validated documents and Subject identity information to

provide additional certificate products that require the same validated information, provided that the documents are still considered valid at the time of re-use.

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 with the Issuing CA. This can be proved by submitting a PKCS #10 Certificate Signing Request (CSR) signed using the private key.

In the case where key generation is performed under the CA or RA's direct control, proof of possession is not required.

3.2.2 Authentication of Organization Identity and Domain Identity

Where an organization identity is included in the Certificate, Applicants are required to provide the organization's name and registered or trading address. The legal existence, legal name, legal form (where included in the request or part of the legal name in the jurisdiction of incorporation) and provided address of the organization must be verified according to methods described in the CPS, and in accordance with Section 3.2.2.1/3.2.2.2 of the Baseline Requirements.

For all SSL/TLS Certificates, the Applicant's ownership or control of all requested Fully Qualified Domain Name(s) must be verified according to methods described within the CPS, and in accordance with Section 3.2.2.4 of the Baseline Requirements.

Further information may be requested from the Applicant and other information and or methods may be utilized in order to achieve an equivalent level of confidence.

3.2.3 Authentication of Individual identity

TrustFactory CAs must issue client end entity certificates, and individual identity must be verified according to methods described within the CPS of the applicable Issuing CA CPS together with the respective TrustFactory RA Charter for Individual Certificates, where applicable In the case where an external RA is involved, RAs shall authenticate individuals using criteria specified in the CPS and TrustFactory RA Charter that depends upon the type of Client Certificate and level of assurance required.

3.2.3.1 Enterprise Registration Authority Authentication

For enterprise or managed services accounts where an Enterprise Registration Authority has been deployed, TrustFactory Issuing CAs and RAs may set authenticated organizational details in the form of an Organization Certificate Profile. Suitably authenticated account administrators, or AOR, acting in the capacity of an Enterprise Registration Authority (ERA) must authenticate individuals affiliated with the organization and issue Certificates based on the Organization Certificate Profile.

3.2.4 Non Verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

Before issuing certificates that assert organizational authority, the CA must validate the subscriber's authority to act in the name of the organization.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

TrustFactory Root CAs must not support re-key or re-issue unless it has been specifically authorized by the PA.

TrustFactory Issuing CAs may support re-key requests from Subscribers prior to the expiry of the Subscriber's existing Certificate. TrustFactory Issuing CAs may also support reissue prior to the expiry of the Certificate.

3.3.1 Identification and Authentication for Routine Re-key

For re-key of any subscriber certificate issued under this certificate policy, identity must be established through log in to the Subscriber Management Portal, Portal API or use of current signature key.

If at any point any Subject name information in a Certificate is changed in any way, the identity proofing procedures for a new certificate outlined in 3.2 above shall be re-performed and a new Certificate issued with the validated information.

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

TrustFactory Issuing CAs must not re-key a Certificate without additional authentication if doing so would allow the Subscriber to use the Certificate beyond its usage limits.

3.3.2 Identification and Authentication for Re-key after Revocation

A routine re-key after revocation is not permitted. After a Certificate has been revoked, the Subscriber shall be required to go through the initial registration process described under Section 3.2 in this CP to obtain a new Certificate.

3.4 Identification and Authentication for Revocation Request

All revocation requests must be authenticated by a TrustFactory RA. Revocation requests may be received from the Subscriber (including designated AOR), the administrative contact of the RA or an ERA.

Revocation requests from Subscribers shall be granted if initiated after logging into the Subscriber Management Portal or received via the TrustFactory API.

A TrustFactory CA may, at its own discretion, also perform revocation of Subscriber certificates in accordance with the requirements of the applicable Subscriber Agreement.

4 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

The Certificate application process must provide sufficient information (as per Section 3.2) to:

- Establish and record identity of the applicant.
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required.
- Establish the applicant's authorization (by the employing or sponsoring organization) to obtain a certificate.
- Verify any role or authorization information requested for inclusion in the certificate.

These steps may be performed in any order that is convenient for the CA and applicants that does not compromise security, but all must be completed before certificate issuance.

4.1.1 Who Can Submit a Certificate Application

A certificate application may be submitted to the CA by the Subscriber, AOR, Trusted Agent or an RA on behalf of the Subscriber.

Approved parties, external RAs may submit certificate applications via a trusted path and the RA is identified using a strong authentication mechanism. This is generally achieved via a secure API.

TrustFactory CAs may maintain their own blacklists for individuals from whom or entities from which they shall not accept Certificate applications. Criteria for adding a Subscriber/Applicant to a Blacklist is at the sole discretion of the management of the TrustFactory Issuing CA.

4.1.2 Enrollment Process and Responsibilities

TrustFactory CAs or RAs must maintain systems and processes that sufficiently authenticate the Applicant's identify for all Certificate types that present the identity to Relying Parties.

Prior to the issuance of a Certificate, the TrustFactory CAs or RAs must obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic;
2. An executed Subscriber Agreement or Terms of Use, which may be electronic; and
3. Any additional documentation requested by TrustFactory CAs or RAs to successfully perform the required verification.

The certificate request must contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

TrustFactory CAs or RAs shall protect communications and securely store information presented by the Applicant during the application process.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

TrustFactory CAs shall establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant, in compliance with its CPS. Initial identity validation shall be performed by the TrustFactory CAs validation team or by Registration Authorities under contract as specified in Section 3.2 of this CP.

All communications shall be securely stored along with all information presented by the Applicant during the application process. Future identification of repeat Applicants and subsequent authentication checks may be addressed through the Subscriber Management Portal, or Portal API, following successful login and authentication.

An Issuing CA issuing publicly trusted SSL/TLS server certificates shall state in its CPS its practices on processing CAA records for Fully Qualified Domain Names (FQDN). Issuing CA's must specify the domain names authorizing issuance in their CPS.

4.2.2 Approval or Rejection of Certificate Applications

TrustFactory CAs must reject applications for Certificates where validation of all items required in the certificate cannot be successfully completed, with the exception of the Organization Unit (OU) field.

Assuming all validation steps can be completed successfully following appropriate techniques TrustFactory CAs may approve the Certificate Request.

TrustFactory CAs may reject applications including for the following reasons:

- If there may be a potential for negative consequences to TrustFactory's brand, reputation or operations in accepting the request.
- For Certificates from Applicants who have previously been rejected or have previously violated a provision of a Subscriber Agreement.
- The Certificate Request is deemed to be High Risk
- Where, TrustFactory, in its sole discretion, considers that the certificate will not be legally compliant for the intended use

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

TrustFactory Issuing CAs shall accept certificate requests directly through the Subscriber Management Portal or Portal APIs, from RAs approved by the TrustFactory PA to perform validation. RAs directly operated by the TrustFactory CA or RAs contracted by the TrustFactory CA shall ensure that all information sent to the CA is verified and authenticated in a secure manner. Certificate issuance may only occur after all required validation has successfully completed.

Certificate issuance by the TrustFactory Root CA requires an individual in a Trusted Role to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

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. Upon the issuance of a Certificate, the Issuing CA must send an email to the Subscriber directing them 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

TrustFactory CAs may deem a Certificate to be accepted, after seven days from issuance of the Certificate, by the Subscriber.

4.4.2 Publication of the Certificate by the CA

TrustFactory CAs may publish a Certificate as follows:

1. Subscriber certificates: by making the Certificate available to the Subscriber or an authorized person acting on behalf of the subscriber
2. CA certificates: by publishing in a Repository at https://www.trustfactory.net/repository

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Issuance status information shall be made available to RAs or local RAs over the TrustFactory API, if they were involved in the initial enrollment.

The TrustFactory Root CA and Issuing CA Certificates must be disclosed to the public by publishing in the Repository on the TrustFactory website at https://www.trustfactory.net/repository.

There is no mandatory requirement to notify other entities.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

TrustFactory CAs must provide a Subscriber Agreement which specifies the obligations of the Subscriber with respect to Private Key protection and avoiding disclosure to third parties. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as 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

TrustFactory CAs must describe the conditions under which Certificates may be relied upon by Relying Parties within their CPS including the appropriate mechanisms available to verify Certificate validity (e.g. CRL or OCSP). Certificates may specify restrictions on use through critical certificate extensions, including the basic constraints, key usage and extended key usage extensions.

Relying Parties should use the information to assess the risk and to ensure suitability of usage and assurances made prior to relying on the Certificate.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Certificate renewal is the process of issuing a new Certificate that has the same subject details and public key as a previously issued Certificate, but with a new validity period.

A TrustFactory CA may renew a Certificate so long as:

- The original Certificate and Public Key is still valid (i.e. has not been revoked or has not expired);
- The Subscriber or subject has not been blacklisted for any reason; and
- All details within the Certificate remain accurate and no new or additional validation is required.

TrustFactory CAs may renew Certificates which have either been previously renewed or previously re-keyed (subject to the points above). The original Certificate should be revoked after renewal is complete.

For all TrustFactory CAs, an email must be generated and sent an email notifying the Subscriber of the need for renewal of their certificate, at least 28 days before the expiry date. The email must be sent to the registered subscriber email address.

4.6.2 Who May Request Renewal

A TrustFactory CA may accept a renewal request provided that it is authorized by the original Subscriber. A renewal request may be accepted from a trusted agent or AOR who retains responsibility for the Private Key on behalf of a Subscriber.

For all CAs and OCSP responders operating under this policy, the corresponding operating authority (TrustFactory General Manager) may request renewal of its own certificate.

4.6.3 Processing Certificate Renewal Requests

Certificate renewal requests must be authenticated.

TrustFactory Issuing CAs may permit Certificate renewal prior to the expiry of the Subscriber's existing Certificate. Subscriber identity is established through authentication to the Subscriber Management Portal.

TrustFactory CAs may reuse, where applicable, previously validated subject and identity information to renew a certificate. If the validation documents are expired or are no longer applicable, then the affected subject and identify information shall be re-validated according to the initial validation procedure

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

A Certificate Re-Key is defined as the process to generate a new Certificate but only allows change to the certificate's public key, no other information may be changed.

A Certificate Re-Issue is defined as the process to generate a new Certificate but only allows change to the certificate's subject alternate name field, no other information may be changed.

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

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

TrustFactory CAs may re-key Certificates which have either been previously renewed or previously re-keyed (subject to the points above). The original Certificate should be revoked after re-key is complete.

4.7.2 Who May Request Certification of a New Public Key

A TrustFactory CA may accept a Re-Key request provided that it is authorized by either the original Subscriber, Trusted agent, partner, or an AOR who retains responsibility for the Private Key, and is suitably authenticated, through the Subscriber Management Portal or through Portal API.

4.7.3 Processing Certificate Re-Key Requests

TrustFactory CAs may reuse, where applicable, previously validated subject and identity information to re-key a certificate. If the validation documents are expired or are no longer applicable then the affected subject and identify information shall be re-validated according to the initial validation procedure.

Subscriber authentication through the Subscriber Management Portal is acceptable and a CSR with a new/different Public Key is mandatory.

The new Public Key must be checked to ensure Key Quality requirements are met.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per 4.4.1

4.7.6 Certificate Publication of the Re-Keyed Certificate by the CA

As per 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

A Certificate Re-Issue is defined as the process to generate a new Certificate where change to the certificate's subject field is allowed, Subscribers are permitted to submit an unlimited number of requests to re-issue any valid Certificate during the validity period of the Certificate

4.8.2 Who May Request Certificate Modification

A TrustFactory CA may accept a Re-Issue request provided that it is authorized by either the original Subscriber, Trusted agent, or an AOR who may retain responsibility for the Private Key, and is suitably authenticated

4.8.3 Processing Certificate Modification Requests

TrustFactory CAs may reuse, where applicable, previously validated subject and identity information to reissue a certificate. If the validation documents are expired or are no longer applicable, validation procedures stipulated in 3.2. shall be followed.

Subscriber authentication through the Subscriber Management Portal or Portal API is accepted.

Notification of New Certificate Issuance to Subscriber as per 4.3.2.

4.8.4 Conduct Constituting Acceptance of a Modified Certificate

As per 4.4.1

4.8.5 Certificate Publication of the Modified Certificate by the CA

As per 4.4.2

4.8.6 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.9 Certificate Revocation and Suspension

Certificate revocation is a process to cancel or retire a certificate by adding the serial number and the date of the revocation to a CRL and publishing the CRL to a repository.

4.9.1 Circumstances for Revocation

A certificate must be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Privilege attributes asserted in the subscriber's certificate are reduced.
- The subscriber can be shown to have violated the stipulations of its subscriber agreement.
- There is reason to believe the private key has been compromised.
- The subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.

The TrustFactory CA's CPS must describe the specific circumstances for revocation as applicable to that CA. Whenever a revocation circumstance occurs, the associated certificate must be revoked and placed on the CRL. Revoked certificates must be included on all new publications of the certificate status information until the certificates expire.

The CRL itself must be digitally signed with the same Private Key which originally signed the Certificate to be revoked.

4.9.2 Who Can Request Revocation

TrustFactory CAs and RAs must accept properly authorized revocation requests from either the RA, Subscriber, authorized person to act on behalf of subscriber, or the AOR of an organization named in the certificate. In the case of TrustFactory CA certificates, the TrustFactory PA can request the revocation. TrustFactory CAs may also at their own discretion revoke Certificates. Furthermore, a TrustFactory CA may revoke a certificate, in its sole discretion, where it considers the certificate not to be legally compliant for the intended use.

The AOR of the organization that owns or controls a device may request the revocation of the device's certificate.

Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties must be able to submit Certificate Problem Reports to the relevant TrustFactory CA.

4.9.3 Procedure for Revocation Request

TrustFactory CAs and RAs shall provide automated mechanisms for requesting and authenticating revocation requests, such as the Subscriber Management Portal for subscribers and the secure API for RAs and partners. RAs may also provide manual backup processes in the event that automated revocation methods are not possible.

TrustFactory CAs and/or RAs must record and authenticate each request for revocation and revoke the Certificate if the request is authentic and approved. A revocation request to revoke a TrustFactory CA Certificate must first be approved by the TrustFactory PA.

Revocation requests must be processed according the procedures defined within the relevant TrustFactory CA's CPS.

The TrustFactory CAs must allow Subscribers, Relying Parties, Application Software Suppliers, and other third parties to submit Certificate Problem Reports, e.g. reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates.

4.9.4 Revocation Request Grace Period

Revocation requests shall be made as soon as reasonably practicable.

4.9.5 Time Within Which CA Must Process the Revocation Request

TrustFactory CAs shall 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 must work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate should be revoked, and if so, a date at which the CA shall revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation shall not exceed the time frames stipulated in the relevant CA CPS document.

The date selected for revocation considers 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 CAs shall revoke certificates as quickly as is practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests received within twelve hours of CRL issuance.

4.9.6 Revocation Checking Requirements for Relying Parties

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 may 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.

4.9.7 CRL Issuance Frequency

Each TrustFactory CA CPS shall document the CRL issuance frequency pertaining to that CA (for Root or Online CA).

4.9.8 Maximum Latency for CRLs

Each TrustFactory CA CPS must document the time within which the CRL will be posted to the repository (for Root or Online CA).

4.9.9 On-Line Revocation/Status Checking Availability

OCSP responses must conform to RFC6960 and/or RFC5019. OCSP responses must either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

4.9.10 On-Line Revocation Checking Requirements

Relying Parties must confirm revocation status information of a certificate on which he/she/it wishes to rely, as per 4.9.6.

For the status of Subscriber Certificates:

- The TrustFactory Issuing CAs shall update information provided via an Online Certificate Status Protocol at least every 24 hours. OCSP responses from this service have a maximum expiration time of ten days.
- If the OCSP responder receives a request for status of a certificate that has not been issued by the TrustFactory Issuing CA, then the responder shall not respond with a "good" status.

For the status of Issuing CA Certificates:

- The TrustFactory Root CAs shall update information provided via a CRL at least
  - (i) every twelve months, and
  - (ii) within 24 hours after revoking a Subordinate CA Certificate.

4.9.11 Other Forms of Revocation Advertisements Available

A Subscriber must be notified of the revocation of a Certificate.

For Issuing CA Certificate revocation, the Policy Authority must be notified when the revocation is completed and a notice must be placed on the Repository.

4.9.12 Special Requirements Related to Key Compromise

Where TrustFactory determines that the CA Private Key may have been Compromised, the TrustFactory Issuing CAs and related RAs shall use commercially reasonable methods (such as an email notification) to inform Subscribers of the potential key compromise.

Where compromise is confirmed the CA Certificate and all issued Subscriber Certificates shall be revoked.

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of TrustFactory CA issued certificates must be available via a CRL distribution point or an OCSP responder or both. The URLs for these services must be made available to Relying Parties within the Certificate.

Revocation entries on a CRL or OCSP Response must not be removed until after the Expiry Date of the revoked Certificate.

CRLs must be signed by the same TrustFactory Issuing CA Private Key that signed the subscriber certificates.

4.10.2 Service Availability

The CA shall operate and maintain its CRL and OCSP capability with sufficient resources to provide a response time of ten seconds or less under normal operating conditions

The TrustFactory CAs shall maintain an online 24x7 service that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

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

4.10.3 Operational Features

No stipulation

4.11 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 must never be escrowed.

TrustFactory CAs must not offer subscriber key escrow services.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable

5 Facility, Management, and Operational Controls

TrustFactory's information security management system must be designed to ensure the following:

- that information assets are appropriately protected
- that users are aware of the importance of information security in the organization
- that the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes is protected
- reducing the damage caused by potential incidents
- ensure the continuity of key and certificate management operations is maintained

TrustFactory's information security management system incorporates and complies with the CA/Browser Forum's Network and Certificate System Security Requirements.

5.1 Physical Controls

All TrustFactory CA equipment, including cryptographic modules, must be protected from theft, loss, physical damage and unauthorized access at all times. TrustFactory CAs must operate under physical and environmental security policies and procedures designed to provide reasonable assurance of the detection, deterrence and prevention of unauthorized logical or physical access to CA related facilities.

5.1.1 Site Location and Construction

TrustFactory Issuing CAs must ensure that the facilities housing the CA hardware as well as software are housed in secure areas with appropriate security barriers and entry controls

5.1.2 Physical Access

TrustFactory CAs and RAs must ensure that the facilities used for CA operations and RA operations are operated in an environment that physically protects the operations from compromise through unauthorized access to systems or data. All TrustFactory facility entrances and exits must be secured and monitored by security personnel, reception staff, or monitoring/control systems.

5.1.3 Power and Air Conditioning

TrustFactory's Issuer CA and RA must maintain a backup power supply and sufficient environmental controls to protect the CA systems and allow the CA to automatically finish pending operations before a lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

The Issuer CA and RAs shall protect equipment from water exposure.

5.1.5 Fire Prevention and Protection

The Issuer CA and RAs shall use facilities equipped with fire suppression mechanisms.

5.1.6 Media Storage

Issuer CAs and RAs shall protect all media from accidental damage, environmental hazards, and unauthorized physical access. Each Issuer CA and each RA shall duplicate and store its audit archive information in a backup location that is separate from its primary operations facilities.

5.1.7 Waste Disposal

TrustFactory CAs shall ensure that all media used for the storage of information is securely erased or destroyed in a generally accepted manner before being released for disposal.

5.1.8 Off-Site Backup

The Issuer CA or RA shall make weekly system backups to aid in recovery from system failure and securely store the backups, including at least one full backup copy, at an offsite location that has procedural and physical controls that are commensurate with its operational location.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

The operational trusted roles shall be the roles fulfilling the following functions:

- Validation Specialist / RA Operator:
  - responsible for approving issuance and revoking certificates
  - performs the Applicant/Subscriber information validation and verification duties
- Auditor:
  - reviewing of CA system audit logs
  - performing compliance checking of operational processes against the CP and CPS
- Security Officer:
  - overall responsibility for administering the CA's information security management system policies and processes
  - PKI systems asset management
  - key ceremony: script compliance, protection of key materials
- Systems Administrator:
  - installation, configuration and maintenance of the CA server and network systems
  - monitoring the operational health of CA systems
  - day-to-day operation, backup and recovery of CA systems
  - administration of the server operating systems and network components
  - preparing and physically operating the HSM appliance and related equipment (host server and attached workstations) for the key ceremony.
  - installing the server and HSM appliance into the vault after the ceremony.
  - Administrative duties on the HSM under a 2-person (dual custody) rule
- CA Administrator:
  - CA cryptographic key life cycle management functions
  - Setup and configuration of CA software
  - overall management and coordination of CA functions

Key Ceremony only trusted roles:

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

- Normal Crypto User:
  - signing operations in key ceremony

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

The CA shall maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in trusted roles and shall make them available during compliance audits.

The RA shall maintain lists, including names, organizations, and contact information of those who act in RA Operations Staff, RA Administrators, and RA Security Officer roles for that RA.

5.2.2 Number of Persons Required per Task

Policy and control procedures must be in place to ensure segregation of duties. Where this is not possible a multi person approach, with those holding trusted roles only should be adopted to perform critical and sensitive tasks.

5.2.3 Identification and Authentication for Each Role

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

All trusted roles require multi-factor authentication.

5.2.4 Roles Requiring Separation of Duties

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

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

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

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

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

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

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

5.3.2 Background Check Procedures

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

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

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

5.3.3 Training Requirements

TrustFactory CAs must ensure that all personnel performing duties with respect to the operation of the CA receive the required training to perform their job responsibilities competently and satisfactorily with regards to:

- basic Public Key Infrastructure knowledge,
- authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement),
- information security policies and processes (including awareness of threats),
- CA operational procedures,
- duties they are expected to be performed, and
- business continuity procedures

5.3.4 Retraining Frequency and Requirements

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

Refresher training shall be conducted as and when required.

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

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

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

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

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

TrustFactory CAs and each Delegated Third Party shall ensure all events relating to the following events are logged in a manner to ensure the traceability to a person in a trusted role for any action required for CA services:

1. CA key lifecycle management events
2. CA and Subscriber Certificate lifecycle management events
3. Security events

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

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

Details of specific events recorded must be listed in each TrustFactory CA's CPS document.

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed according to a regular schedule and documented process. Unauthorized or suspicious activity detected during the reviews must be investigated.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained for at least seven years or held for a longer period of time as appropriate to provide necessary evidence in accordance with any applicable legislation.

5.4.4 Protection of Audit Log

The audit logs shall be protected in a manner to ensure they cannot be deleted or destroyed (except for transfer to long term media) for the duration of their retention period. Only authorized trusted individuals shall be able to perform any operations related to the audit logs. The records of events shall be date stamped in a secure manner.

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

5.4.5 Audit Log Backup Procedures

TrustFactory CAs and RAs shall ensure that audit logs are backed-up to a secure off-site location, under the control of an authorized trusted role, and that the audit log backup data should be protected to the same degree as production data.

5.4.6 Audit Collection System (Internal vs. External)

No stipulation.

5.4.7 Notification to Event-Causing Subject

No stipulation .

5.4.8 Vulnerability Assessments

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

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

Each Delegated Third Party (or RA) shall perform similar vulnerability assessments and penetration tests on their Certificate systems.

Additionally, the TrustFactory's security program must include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

5.5 Records Archival

5.5.1 Types of Records Archived

TrustFactory CAs and RAs must archive records with enough detail to establish the validity of a signature and of the proper operation of the CA system. All records related to auditable events defined in Section 5.4.1 shall be archived.

5.5.2 Retention Period for Archive

The TrustFactory CAs and Delegated Third Parties (or RAs) must retain all documentation relating to certificate requests and the verification thereof, and all Certificates issued and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

Both archive data and archive storage media must be protected. Protection measures must ensure that only authorized trusted roles have access to operate on the archive and that the integrity and confidentiality of the archive data is maintained. Secure mechanisms must be used to periodically transfer the archived data to new media so that records are retrievable and readable throughout the period of time for which they are required to be held.

5.5.4 Archive Backup Procedures

The Issuer CA or RA must describe how its records are backed up and managed in its CPS or a referenced document.

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

All archive records must be collected from internal systems and processes.

5.5.7 Procedures to Obtain and Verify Archive Information

The applicable CPS must describe procedures to obtain and verify archive information.

5.6 Key Changeover

The applicable CPS must describe the procedures for CA key changeover.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The Issuer CA must implement and document procedures to be followed in the event of a serious security incident or system compromise.

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

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

5.7.3 Recovery Procedures After Key Compromise

If a TrustFactory Issuing CA suspects that a CA Private Key is compromised or lost then the Issuing CA shall follow its Incident Response Plan. If there is a compromise or loss, the Issuer CA shall notify any affiliated entities so that they may issue CRLs revoking cross-Certificates issued to the Issuer CA and shall notify interested parties and make information available that can be used to identify which Certificates were affected, unless doing so would breach the privacy of the Issuer CA's user or the security of the Issuer CA's services.

5.7.4 Business Continuity Capabilities after a Disaster

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

5.8 CA or RA Termination

The TrustFactory Policy Authority is the body authorized to terminate a TrustFactory Root CA or TrustFactory Issuing CA for any reason whatsoever. The TrustFactory CA shall document in its CPS the procedures it follows during CA or RA termination.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

TrustFactory Root and Issuing CAs shall:

1. generate their CA keys in a physically secured environment as described in Section 5.1;
2. generate their CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. generate their CA keys within cryptographic modules meeting the applicable technical and business requirements as specified in Section 6.2;
4. log their CA key generation activities; and
5. maintain effective controls to provide reasonable assurance that their Private Keys were generated and protected in conformance with the procedures described in the Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

For CA Key Pairs created for CAs operated and controlled by the TrustFactory organization (which operates the Root CA), the CA shall:

1. prepare and follow a Key Generation Script and
2. have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process.
3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

The Issuing CA shall reject a subscriber certificate request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key.

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in FIPS 140 Level 3 validated cryptographic modules.

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subscriber Key Pair Generation

For Subscriber keys generated by issuing CA, Key generation must be performed in a secure cryptographic device that meets FIPS 140-2 (or equivalent) using key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6.

6.1.2 Private Key Delivery to Subscriber

TrustFactory CAs and RAs do not deliver subscriber private keys.

6.1.3 Public Key Delivery to Certificate Issuer

TrustFactory CAs shall only accept Public Keys from Subscribers that are delivered 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 CAs shall ensure that its Public Keys are delivered to Relying Parties in such a way as to prevent substitution attacks.

TrustFactory CA Public Keys shall be made publicly available.

TrustFactory CA shall work with commercial browsers and platform operators to embed Root Certificate Public Keys into root stores and operating systems.

6.1.5 Key Sizes

Certificates shall meet the following requirements for algorithm type and key size as defined by Baseline Requirements:

Root CA 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

Subordinate CA 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

Subscriber Certificates (including infrastructure certificates)

Digest algorithm	SHA- 256, SHA-384 or SHA- 512
RSA modulus size (bits)	Minimum 2048 bits and must be divisible by 8
ECC curve	NIST P-256 or P-384 or P-521

6.1.6 Public Key Parameters Generation and Quality Checking

TrustFactory CAs shall generate Key Pairs in accordance with the Baseline Requirements and shall use reasonable techniques to validate the suitability of Public Keys presented by Subscribers. The quality of the generated Key Parameters shall be verified in accordance with Baseline Requirements.

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

TrustFactory CAs shall set key usage of Certificates depending on their proposed field of application via the v3 Key Usage Field for X.509 version 3.

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The TrustFactory CAs shall implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key.

The TrustFactory CAs shall encrypt their Private Key with an algorithm and key-length that meets current strength requirements (2048-bit minimum). TrustFactory CAs shall ensure that Hardware Security Modules that have been activated are not left unattended and are protected from unauthorized access.

6.2.1 Cryptographic Module Standards and Controls

TrustFactory Root and Issuing CAs shall ensure that all systems signing Certificates and CRLs or generating OCSP responses use FIPS 140-2 level 3 as the minimum level of cryptographic protection. Issuing CAs that require

Subscribers to use FIPS 140-2 level 2 or above systems for Private Key protection must contractually obligate the Subscriber to use such a system or provide a suitable mechanism to guarantee protection.

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

TrustFactory Root and Issuing CAs shall activate Private Keys for cryptographic operations with multi-person control, using people in trusted roles. The trusted roles that operate the multi-person controls are authenticated using token and PIN code.

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

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

6.2.3 Private Key Escrow

TrustFactory Root and Issuing CAs do not escrow Private Keys.

6.2.4 Private Key Backup

TrustFactory Root and Issuing CAs shall back up Private Keys for disaster recovery purposes using the same multi-person control as the original Private Key generation.

Two backups shall be created. One backup shall be stored at the primary site and one backup at the disaster recovery (DR) site.

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

TrustFactory CAs do not perform backups of Subscriber Private keys

6.2.5 Private Key Archival

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

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

TrustFactory CAs do not perform archival of Subscriber Private keys

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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

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

6.2.7 Private Key Storage on Cryptographic Module

TrustFactory CAs shall store CA Private Keys on minimum least a FIPS 140-2 level 3 Hardware Security Modules.

6.2.8 Method of Activating Private Key

TrustFactory CAs shall be responsible for activating the Private Key, during a key ceremony, in accordance with the instructions and documentation provided by the manufacturer of the Hardware Security Module.

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).

6.2.9 Method of Deactivating Private Key

The CA must document in its CPS the procedures followed when deactivating a Private Key.

The TrustFactory PA must authorize any CA Private Key deactivation.

6.2.10 Method of Destroying Private Key

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

The TrustFactory CA shall document in its CPS the procedures followed when destroying a Private Key.

The TrustFactory PA must authorize any CA Private Key destruction.

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

TrustFactory CAs must archive Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

CA Private Keys and Certificates and renewed Certificates shall have a maximum validity period as per table below:

	Client	SSL
Root CA	Up to 30 years	Up to 30 years
Subordinate CA	Up to 15 years	Up to 15 years
Issuing CA	Up to 15 years	Up to 15 years
Subscriber	Up to 3 years	Up to 1 year

In some cases, the maximum validity period may not be realized by the Subscriber in the event the current or future Baseline Requirements impose requirements on Certification Authorities relative to Certificate issuance that were not in place at the time the Certificate was originally issued. Particularly in the case of a request for reissuance, e.g., additional requirements are included for identification and authentication for certain Certificate type, or maximum Validity Period is decreased.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

TrustFactory CA activation data used to activate TrustFactory CA Private Keys shall be generated during a key ceremony. Activation data shall be 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 CA activation data shall be 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 CA activation data shall only be held by personnel in trusted roles.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The CA shall document its Computer Security Technical Requirements in its CPS.

All user accounts capable of directly causing certificate issuance shall be protected by multi-factor authentication.

6.5.2 Computer Security Rating

No Stipulation

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

The configuration of the TrustFactory CA system as well as any modifications and upgrades shall be documented and controlled by the TrustFactory CA management.

6.6.3 Lifecycle Security Controls

No stipulation.

6.7 Network Security Controls

TrustFactory CA shall implement appropriate security measures to protect against network based attacks and vulnerabilities.

6.8 Timestamping

No stipulation.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

TrustFactory CAs shall meet the technical requirements set forth in Section 2.2 – Publication of Information, Section 6.1.5 – Key Sizes, and Section 6.1.6 – Public Key Parameters Generation and Quality Checking.

TrustFactory Issuing CAs shall generate non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1 Version Number(s)

TrustFactory CAs shall issue Certificates in compliance with X.509 Version 3.

7.1.2 Certificate Content and Extensions

TrustFactory CAs shall issue Certificates in compliance with RFC 5280 and meet the requirements for Certificate content and extensions as specified in the Baseline Requirements.

7.1.2.1 Root CA Certificate

The relevant TrustFactory Root CA CPS document shall specify details of Root CA Certificate profiles.

7.1.2.2 Subordinate CA Certificate

The relevant TrustFactory Root CA CPS document shall specify details of Issuing CA Certificate profiles.

7.1.2.3 Subscriber Certificates

The relevant TrustFactory Issuing CA CPS document shall specify details of Subscriber Certificate profiles.

7.1.2.4 All Certificates

All other fields and extensions must be set in accordance with RFC 5280.

7.1.3 Algorithm Object Identifiers

7.1.3.1 SubjectPublicKeyInfo

The following requirements apply to the subjectPublicKeyInfo field within a TrustFactory Certificate or Precertificate.

No other encodings are permitted.

7.1.3.1.1 RSA

The CA shall indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters must be present, and must be an explicit NULL.

The CA shall not use a different algorithm, such as the id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) algorithm identifier, to indicate an RSA key.

When encoded, the AlgorithmIdentifier for RSA keys must be byte-for-byte identical with the following hex-encoded bytes:

```
30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00
```

7.1.3.1.2 ECDSA

The CA shall indicate an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters must use the namedCurve encoding.

For P-256 keys, the namedCurve must be secp256r1 (OID: 1.2.840.10045.3.1.7).

For P-384 keys, the namedCurve must be secp384r1 (OID: 1.3.132.0.34).

For P-521 keys, the namedCurve must be secp521r1 (OID: 1.3.132.0.35).

When encoded, the AlgorithmIdentifier for ECDSA keys must be byte-for-byte identical with the following hex-encoded bytes:

ECDSA Keys	AlgorithmIdentifier Hex Encoding
P-256 keys	30 13 06 07 2a 86 48 ce 3d 02 01 06 08 2a 86 48 ce 3d 03 01 07
P-384 keys	30 10 06 07 2a 86 48 ce 3d 02 01 06 05 2b 81 04 00 22
P-521 keys	30 10 06 07 2a 86 48 ce 3d 02 01 06 05 2b 81 04 00 23

TrustFactory CAs must not issue any Subscriber certificates or CA certificates using the SHA-1 algorithm.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by a CA Private Key must conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures,

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

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

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

The CA shall use one of the following signature algorithms and encodings.

When encoded, the AlgorithmIdentifier must be byte-for-byte identical with the following specified hex-encoded bytes:

Algorithm	AlgorithmIdentifier Hex Encoding
RSASSA-PKCS1-v1_5 with SHA-256	30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00
RSASSA-PKCS1-v1_5 with SHA-384	30 0d 06 09 2a 86 48 86 f7 0d 01 01 0c 05 00
RSASSA-PKCS1-v1_5 with SHA-512	30 0d 06 09 2a 86 48 86 f7 0d 01 01 0d 05 00
RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes	30 41 06 09 2a 86 48 86 f7 0d 01 01 0a 30 34 a0 0f 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 a1 1c 30 1a 06 09 2a 86 48 86 f7 0d 01 01 08 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 a2 03 02 01 20

RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes	30 41 06 09 2a 86 48 86 f7 0d 01 01 0a 30 34 a0 0f 30 0d 06 09 60 86 48 01 65 03 04 02 02 05 00 a1 1c 30 1a 06 09 2a 86 48 86 f7 0d 01 01 08 30 0d 06 09 60 86 48 01 65 03 04 02 02 05 00 a2 03 02 01 30
RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes	30 41 06 09 2a 86 48 86 f7 0d 01 01 0a 30 34 a0 0f 30 0d 06 09 60 86 48 01 65 03 04 02 03 05 00 a1 1c 30 1a 06 09 2a 86 48 86 f7 0d 01 01 08 30 0d 06 09 60 86 48 01 65 03 04 02 03 05 00 a2 03 02 01 40

In addition, the CA may use these signature algorithms and encodings if all of the following conditions are met:

- If used within a Certificate, such as the signatureAlgorithm field of a Certificate or the signature field of a TBSCertificate:
  - The new Certificate is a Root CA Certificate or Subordinate CA Certificate that is a Cross-Certificate; and
  - There is an existing Certificate, issued by the same issuing CA Certificate, using the following encoding for the signature algorithm; and
  - The existing Certificate has a serialNumber that is at least 64-bits long; and
  - The only differences between the new Certificate and existing Certificate are one of the following:
    - A new subjectPublicKey within the subjectPublicKeyInfo, using the same algorithm and key size; and/or,
    - A new serialNumber, of the same encoded length as the existing Certificate; and/or
    - The new Certificate's extKeyUsage extension is present, has at least one key purpose specified, and none of the key purposes specified are the id-kp-serverAuth (OID: 1.3.6.1.5.5.7.3.1) or the anyExtendedKeyUsage (OID: 2.5.2937.0) key purposes; and/or
    - The new Certificate's basicConstraints extension has a pathLenConstraint that is zero.

- If used within an OCSP response, such as the signatureAlgorithm of a BasicOCSPResponse:
  - All unexpired, un-revoked Certificates that contain the Public Key of the CA Key Pair and that have the same Subject Name must also contain an extKeyUsage extension with the only key usage present being the id-kp-ocspSigning (OID: 1.3.6.1.5.5.7.3.9) key usage.

- If used within a CRL, such as the signatureAlgorithm field of a CertificateList or the signature field of a TBSCertList:
  - The CRL is referenced by one or more Root CA or Subordinate CA Certificates; and,
  - The Root CA or Subordinate CA Certificate has issued one or more Certificates using the following encoding for the signature algorithm.

Note: The above requirements do not permit a CA to sign a Pre-certificate with this algorithm and encoding: RSASSA-PKCS1-v1_5 with SHA-1; encoding:

```
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00
```

7.1.3.2.2 ECDSA

The CA shall use the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is P-256, the signature must use ECDSA with SHA-256. When encoded, the AlgorithmIdentifier must be byte-for-byte identical with the following hex-encoded bytes:

```
30 0a 06 08 2a 86 48 ce 3d 04 03 02
```

If the signing key is P-384, the signature must use ECDSA with SHA-384. When encoded, the AlgorithmIdentifier must be byte-for-byte identical with the following hex-encoded bytes:

```
30 0a 06 08 2a 86 48 ce 3d 04 03 03
```

If the signing key is P-521, the signature must use ECDSA with SHA-512. When encoded, the AlgorithmIdentifier must be byte-for-byte identical with the following hex-encoded bytes:

```
30 0a 06 08 2a 86 48 ce 3d 04 03 04
```

7.1.4 Name Forms

7.1.4.1 Issuer Information

TrustFactory CAs shall issue Certificates with name forms compliant to RFC 5280, section 4.1.2.4. 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.

The following requirements shall met by all newly-issued TrustFactory Subordinate CA Certificates that are not used to issue TLS certificates, as defined in Section 7.1.2.2, and shall be met for all other Certificates, regardless of whether the Certificate is a CA Certificate or a Subscriber Certificate.

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

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

7.1.4.2 Subject Information – Subscriber Certificates

By issuing a Certificate, the CA represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. TrustFactory shall be fully complaint with the baseline requirements set out under section 7.1.4.2

7.1.4.2.1 Subject Alternative Name Extension

TrustFactory SSL Subscriber certificates are populated with the Subject fields and criteria according to the following table:

Certificate Field	Criteria
extensions:subjectAltName	**Required.** This extension contains at least one entry. It contains each Fully-Qualified Domain Name (FQDN) that has been validated as per Section 3.2.2.4 or 3.2.2.5. Wildcard FQDNs are permitted. TrustFactory does not issue certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name. Entries in the dNSName are in the "preferred name syntax", as specified in RFC 5280, and thus must not contain underscore characters ("_").

7.1.4.2.2 Subject Distinguished Name Fields

TrustFactory SSL CA shall verify all subscriber subject info that is included in the subject of the cert as per section 3.2.2.2.

Certificate Field	Criteria
subject:commonName (OID 2.5.4.3)	**Optional.** Contains a single Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension
subject:organizationName (OID 2.5.4.10)	**Optional.** Contains Subscriber Organization name or DBA name as verified under Section 3.2.2.2.
subject:localityName (OID: 2.5.4.7)	**Required** if the subject:organizationName, subject:givenName field, or subject:surname field are present and the subject:stateOrProvinceName field is absent. **Optional** if the subject:stateOrProvinceName field and the subject:organizationName subject:givenName field, or subject:surname are present. **Prohibited** if the subject:organizationName, subject:givenName, and subject:surname field are absent. Contains the Subject's locality information as verified under Section 3.2.2.1. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2 (g), the localityName field may contain the Subject's locality and/or state or province information as verified under Section 3.2.2.1.
subject:stateOrProvinceName (OID: 2.5.4.8)	**Required** if the subject:organizationName field subject:givenName field, or subject:surname field are present and subject:localityName field is absent. **Optional** if the subject:localityName field and the subject:organizationName field the subject:givenName field, or the subject:surname field are present. **Prohibited** if the subject:organizationName field, the subject:givenName field, or subject:surname field are absent. Contains the Subject's state or province information as verified under Section 3.2.2.1. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2 (g), the subject:stateOrProvinceName field may contain the full name of the Subject's country information as verified under Section 3.2.2.1.
subject:countryName (OID: 2.5.4.6)	**Required** if the subject:organizationName field subject:givenName, or subject:surname field are present. **Optional** if the subject:organizationName field subject:givenName, or subject:surname field are absent Contains the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.2.1. If a Country is not represented by an official ISO 3166-1 country code, the CA may specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

subject:organizationalUnitName	**Optional.** TrustFactory CA implements a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless it has verified this information in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.
Other subject attributes	Other attributes may be present within the subject field. If present, other attributes must contain information that has been verified by TrustFactory CA.

7.1.5 Name Constraints

TrustFactory shall not currently operate technically constrained Subordinate CAs.

7.1.6 Certificate Policy Object Identifier

The TrustFactory CP and CPS policy object identifiers (OID) are as stated in Section 1.2.

TrustFactory SSL Issuing CA shall issue certificates to Subscribers that comply with the latest version of the CAB Forum Baseline Requirements.

7.1.7 Usage of Policy Constraints Extension

TrustFactory CAs may issue Certificates with a policy qualifier and suitable text to aid Relying Parties in determining applicability.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

TrustFactory CAs shall issue Version 2 CRLs in compliance with RFC 5280.

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 Issuing CAs shall operate an Online Certificate Status Profile (OCSP) responder in compliance with RFC 6960 or RFC5019.

7.3.1 Version Number(s)

TrustFactory Issuing CAs shall issue Version 1 OCSP responses.

7.3.2 OCSP Extensions

Details of the Issuing CA OCSP profile must be documented in the Issuing CA CPS.

8 Compliance Audit and Other Assessments

TrustFactory CA shall ensure that it:

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

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

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

Authorized RAs that provide Advanced Electronic Signature (AES) Certificates shall be audited for compliance to South African Accreditation Authority requirements.

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

TrustFactory shall comply with the South African Protection of Private Information Act (POPIA) requirements.

8.1 Frequency and Circumstances of Assessment

TrustFactory CAs shall complete a compliance audit to ensure compliance with the WebTrust or SAAA standards identified above (where products and services offered require compliance) via a Qualified Auditor on an annual basis at least.

8.2 Identity/Qualifications of Assessor

Applicable audits of TrustFactory CAs shall be performed by a Qualified Auditor.

A Qualified Auditor shall mean a natural person, legal entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

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

8.3 Assessor's Relationship to Assessed Entity

TrustFactory shall choose an auditor/assessor who is completely independent from the TrustFactory CA.

8.4 Topics Covered by Assessment

The audit shall meet the requirements of the following audit scheme(s):

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

Authorized RAs that provide Advanced Electronic Signature (AES) Certificates shall be audited for compliance to South African Accreditation Authority requirements.

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

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

8.5 Actions Taken as a Result of Deficiency

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

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

8.6 Communications of Results

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

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

All TrustFactory CA audit reports shall be published on the Repository.

8.7 Self-Audits

TrustFactory CA shall monitor adherence to its Certificate Policy and Certification Practice Statements and strictly controls its service quality by performing self-audits on at least a quarterly.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

TrustFactory may charge fees for the issuance, management and renewal, of the various Certificate products that it offers. Such fees should be published for applicants and subscribers.

9.1.2 Certificate Access Fees

TrustFactory may charge a fee for access to its databases of issued Certificates.

9.1.3 Revocation or Status Information Access Fees

TrustFactory may charge a fee for access to its published CRLs or OCSP services as described in the applicable CA's CPS.

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

No stipulation

9.2.3 Insurance or Warranty Coverage for End Entities

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

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

9.3.2 Information Not Within the Scope of Confidential Information

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

9.3.3 Responsibility to Protect Confidential Information

TrustFactory CAs shall protect confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

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

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property rights

TrustFactory CAs shall not knowingly violate the intellectual property rights of third parties.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

TrustFactory CAs shall use this CP and applicable Subscriber Agreements to convey legal conditions of usage of

issued Certificates to Subscribers and Relying Parties. Participants that may make representations and warranties include TrustFactory CA, RAs, Subscribers, Relying Parties, and any other participants as it might become necessary. All parties including the TrustFactory CA, any RAs and Subscribers warrant the integrity of their respective Private Key(s). If any such party suspects that a Private Key has been compromised they shall immediately notify the appropriate RA.

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

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

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

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

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

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

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

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

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

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

9.6.2 RA Representations and Warranties

The CA shall require RAs to warrant that:

- Verification and Issuance processes are in compliance with this CP and the relevant TrustFactory CA CPS;
- All information provided to TrustFactory CA does not contain any misleading or false information;
- All translated material provided by the RA is accurate;
- The RAs are not the agents, fiduciaries, trustees, or other representatives of subscribers or relying parties;
- The RA maintains the ability to ensure
    a. the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

b. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
c. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational security measures; and
d. compliance with applicable data protection legislation.

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

9.6.3 Subscriber Representations and Warranties

The CA shall require Subscribers and/or Applicants, of end-entity certificates, to warrant that:

- Subscriber shall provide accurate and complete information at all times to TrustFactory CA, both in the Certificate Request and as otherwise requested by TrustFactory CA in connection with issuance of a Certificate;
- Subscribers and/or Applicant shall take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key to be included in the requested Certificate(s) and any associated activation data or device, e.g. password or token;
- Subscriber shall review and verify the Certificate contents for accuracy;
- For SSL/TLS Certificates, the Subscriber shall install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- Subscriber shall (a) promptly request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate; and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
- Subscriber shall promptly cease use of Private Key associated with the Public Key in the Certificate upon revocation of that Certificate;
- Subscriber shall respond to TrustFactory CA's instructions concerning Compromise or Certificate misuse within forty-eight (48) hours; and
- Applicant acknowledges and accepts that TrustFactory CA is entitled to revoke the Certificate immediately if the Applicant violates the terms of the Subscriber Agreement or Terms of Use or if TrustFactory CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

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

- Information in the Issuing CA Certificate is accurate and complete before publishing it to the Repository;
- All reasonable measures are taken to assure control of, keep confidential, and properly protect at all times the Private Key of the Issuing CA and any associated activation data or device, e.g. password or token;
- The Certificate contents are verified for accuracy;
- The Certificate is used in compliance with all applicable laws and in accordance with this CP and The applicable CA's CPS;
- The Issuing CA Certificate is, within 24 hours, revoked and use of its associated Private Key is terminated, if (a) there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in Certificate; and (b) if any information in the Certificate is or becomes incorrect or inaccurate;

9.6.4 Relying Party Representations and Warranties

The CA may require a party relying on a TrustFactory CA's Certificate to warrant to:

- Have the technical capability to use Certificates;
- Receive notice of the TrustFactory CA and associated conditions for Relying Parties;
- Validate a TrustFactory CA's Certificate by using Certificate status information (a CRL or OCSP) published by the TrustFactory CA in accordance with the proper Certificate path validation procedure;
- Trust a TrustFactory CA's Certificate only if all information featured on such Certificate can be verified via such a validation procedure as being correct and up to date;
- Rely on a TrustFactory CA's Certificate, only as it may be reasonable under the circumstances; and
- Notify the appropriate TrustFactory CA or RA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been compromised.

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

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

- Take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or this CP;
- Take any other precautions prescribed in the TrustFactory CA's Certificate as well as any other policies or terms and conditions made available in the application context a Certificate might be used.

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

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

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

TrustFactory CA does not warrant:

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

9.8 Limitations of Liability

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

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

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

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

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

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber agreements.

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

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

9.9 Indemnities

9.9.1 Indemnification by TrustFactory CA

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

9.9.2 Indemnification by Subscribers

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

9.9.3 Indemnification by Relying Parties

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

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

TrustFactory accepts notices related to this CP and any of its Root CAs CPS's or Issuing CAs CPS's by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from

TrustFactory CA the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows.

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

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

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

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

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

9.12.2 Notification Mechanism and Period

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

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

9.12.3 Circumstances Under Which OID Must be Changed

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

9.13 Dispute Resolution Provisions

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

For disputes arising under, in connection with or relating to this CP or a TrustFactory CPS, complaining parties agree to notify TrustFactory of the dispute in an effort to seek dispute resolution, before resorting to any other resolution mechanism including adjudication, mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice. The Parties shall, at the first instance, attempt to resolve all disputes through discussion in an atmosphere of mutual cooperation. TrustFactory management shall respond to a formal dispute notice within 30 days. In the event of failure to mutually resolve the dispute, the dispute shall be referred to arbitration or an Independent Technical Expert (if the dispute is of a technical nature). The Arbitrator or Independent Technical Expert shall be chosen by the parties by mutual agreement. If the Parties cannot agree on an Arbitrator or Independent Technical Expert, then the dispute shall be finally resolved in accordance with the rules of the Arbitration Foundation of Southern

Africa applicable to international arbitration by an arbitrator appointed by the Foundation. In the event that the parties do not agree to the seat, the Foundation shall select the seat of the arbitration.

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

9.14 Governing Law

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

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

9.15 Compliance with Applicable Law

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

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

Entities operating under this CP must not assign their rights or obligations without the prior written consent of TrustFactory.
Where TrustFactory has provided written consent to assign rights and obligations detailed in this CP and an associated TrustFactory CA CPS (including as a result of merger or a transfer of a controlling interest in voting securities), such assignment should be undertaken consistent with this CP articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.
This CP shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties.

9.16.3 Severability

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

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

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

9.16.5 Force Majeure

Trustfactory is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay

or failure is caused by an occurrence beyond TrustFactory's reasonable control. The operation of the Internet is beyond Trustfactory's reasonable control.

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

9.17 Other Provisions

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

ANNEXURE A RFC 6844 ERRATA 5065

TrustFactory does not process CNAME chains

ANNEXURE B CAA CONTACT TAG

TrustFactory does not allow CAA contact details to be published in the DNS

ANNEXURE C Issuance of Certificates for .onion Domain Names

TrustFactory does not allow this method for domain names