PUBLIC

TrustFactory Certification Authority Certificate Policy

Date: 15 December 2017

Version 1.2

Table of Contents

1 Introduction 8
1.1 Overview 8
1.2 Document Name and Identification 9
1.3 PKI participants 9
1.3.1 Certification Authorities 9
1.3.2 Registration Authorities 9
1.3.3 Subscribers 10
1.3.4 Relying Parties 10
1.3.5 Other Participants 10
1.4 Certificate usage 10
1.4.1 Appropriate Certificate Usage 10
1.4.2 Prohibited Certificate Usage 10
1.5 Policy Administration 10
1.5.1 Organization Administering the Document 10
1.5.2 Contact Person 11
1.5.3 Person Determining CP Suitability for the Policy 11
1.5.4 CP Approval Procedures 11
1.6 Definitions and acronyms 11
2 Publication and Repository Responsibilities 16
2.1 Repositories 16
2.2 Publication of Certificate Information 16
2.3 Time or Frequency of Publication 16
2.4 Access control on repositories 16
3 Identification and Authentication 17
3.1 Naming 17
3.1.1 Types of Names 17
3.1.2 Need for Names to be Meaningful 17
3.1.3 Anonymity or Pseudonymity of Subscribers 17
3.1.4 Rules for Interpreting Various Name Forms 17
3.1.5 Uniqueness of Names 17
3.1.6 Recognition, Authentication, and Role of Trademarks 17
3.2 Initial Identity Validation 17
3.2.1 Method to Prove Possession of Private Key 17
3.2.2 Authentication of Organization and Domain Identity 18
3.2.3 Authentication of Individual identity 18
3.2.4 Non Verified Subscriber Information 18
3.2.5 Validation of Authority 18
3.2.6 Criteria for Interoperation 18
3.3 Identification and Authentication for Renewal Requests 18
3.4 Identification and Authentication for Re-key Requests 18
3.4.1 Identification and Authentication for Routine Re-key 19
3.4.2 Identification and Authentication for Re-key / Re-issue after Revocation 19
3.5 Identification and Authentication for Revocation Request 19
4 Certificate Lifecycle Operational Requirements 20
4.1 Certificate Application 20
4.1.1 Who Can Submit a Certificate Application 20
4.1.2 Enrollment Process and Responsibilities 20
4.2 Certificate Application Processing 20

4.2.1 Performing Identification and Authentication Functions 20
4.2.2 Approval or Rejection of Certificate Applications 20
4.2.3 Time to Process Certificate Applications 21

4.3 Certificate Issuance 21
4.3.1 CA Actions during Certificate Issuance 21
4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate 21

4.4 Certificate Acceptance 21
4.4.1 Conduct Constituting Certificate Acceptance 21
4.4.2 Publication of the Certificate by the CA 21
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 21

4.5 Key Pair and Certificate Usage 21
4.5.1 Subscriber Private Key and Certificate Usage 21
4.5.2 Relying Party Public Key and Certificate Usage 21

4.6 Certificate Renewal 21
4.6.1 Circumstances for Certificate Renewal 21
4.6.2 Who May Request Renewal 22
4.6.3 Processing Certificate Renewal Requests 22
4.6.4 Notification of New Certificate Issuance to Subscriber 22
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 22
4.6.6 Publication of the Renewal Certificate by the CA 22
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 22

4.7 Certificate Re-Key 22
4.7.1 Circumstances for Certificate Re-Key 22
4.7.2 Who May Request Certification of a New Public Key 22
4.7.3 Processing Certificate Re-Keying Requests 23
4.7.4 Notification of New Certificate Issuance to Subscriber 23
4.7.5 Conduct Constituting Acceptance of a Re-Keyed 23
4.7.6 Certificate Publication of the Re-Keyed Certificate by the CA 23
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 23

4.8 Certificate Modification 23

4.9 Certificate Revocation and Suspension 23
4.9.1 Circumstances for Revocation 23
4.9.2 Who Can Request Revocation 23
4.9.3 Procedure for Revocation Request 23
4.9.4 Revocation Request Grace Period 24
4.9.5 Time Within Which CA Must Process the Revocation Request 24
4.9.6 Revocation Checking Requirements for Relying Parties 24
4.9.7 CRL Issuance Frequency 24
4.9.8 Maximum Latency for CRLs 24
4.9.9 On-Line Revocation/Status Checking Availability 24
4.9.10 On-Line Revocation Checking Requirements 24
4.9.11 Other Forms of Revocation Advertisements Available 25
4.9.12 Special Requirements Related to Key Compromise 25
4.9.13 Notification of Certificate Revocation to Subscriber 25
4.9.14 Circumstances for Suspension 25

4.10 Certificate Status Services 25
4.10.1 Operational Characteristics 25
4.10.2 Service Availability 25
4.10.3 Operational Features 25
4.10.4 End of Subscription 25

4.11 Key Escrow and Recovery 25
4.11.1 Key Escrow and Recovery Policy and Practices 25
4.11.2 Session Key Encapsulation and Recovery Policy and Practices 25

5 Facility, Management, and Operational Controls 27

5.1 Physical Controls 27
5.1.1 Site Location and Construction 27
5.1.2 Physical Access 27
5.1.3 Power and Air Conditioning 27
5.1.4 Water Exposures 27
5.1.5 Fire Prevention and Protection 27
5.1.6 Media Storage 27

5.1.7 Waste Disposal 28
5.1.8 Off-Site Backup 28

5.2 Procedural Controls 28
5.2.1 Trusted Roles 28
5.2.2 Number of Persons Required per Task 29
5.2.3 Identification and Authentication for Each Role 29
5.2.4 Roles Requiring Separation of Duties 29

5.3 Personnel Controls 29
5.3.1 Qualifications, Experience, and Clearance Requirements 29
5.3.2 Background Check Procedures 30
5.3.3 Training Requirements 30
5.3.4 Retraining Frequency and Requirements 30
5.3.5 Job Rotation Frequency and Sequence 30
5.3.6 Sanctions for Unauthorized Actions 30
5.3.7 Independent Contractor Requirements 30
5.3.8 Documentation Supplied to Personnel 30

5.4 Audit Logging Procedures 31
5.4.1 Types of Events Recorded 31
5.4.2 Frequency of Processing Log 31
5.4.3 Retention Period for Audit Log 31
5.4.4 Protection of Audit Log 31
5.4.5 Audit Log Backup Procedures 31
5.4.6 Audit Collection System (Internal vs. External) 31
5.4.7 Notification to Event-Causing Subject 31
5.4.8 Vulnerability Assessments 31

5.5 Records Archival 32
5.5.1 Types of Records Archived 32
5.5.2 Retention Period for Archive 32
5.5.3 Protection of Archive 32
5.5.4 Archive Backup Procedures 32
5.5.5 Requirements for Time-Stamping of Records 32
5.5.6 Archive Collection System (Internal or External) 32
5.5.7 Procedures to Obtain and Verify Archive Information 32

5.6 Key Changeover 32

5.7 Compromise and Disaster Recovery 32
5.7.1 Incident and Compromise Handling Procedures 32
5.7.2 Procedures if Computing Resources, Software, and/or Data Are Corrupted 33
5.7.3 Entity Private Key Compromise Procedures 33
5.7.4 Business Continuity Capabilities After a Disaster 33

5.8 CA or RA Termination 34

6 Technical Security Controls 35

6.1 Key Pair Generation and Installation 35
6.1.1 Key Pair Generation 35
6.1.2 Private Key Delivery to Subscriber 35
6.1.3 Public Key Delivery to Certificate Issuer 35
6.1.4 CA Public Key Delivery to Relying Parties 35
6.1.5 Key Sizes 36
6.1.6 Public Key Parameters Generation and Quality Checking 36
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 37

6.2 Private Key Protection and Cryptographic Module Engineering Controls 37
6.2.1 Cryptographic Module Standards and Controls 37
6.2.2 Private Key (m of n) Multi-Person Control 37
6.2.3 Private Key Escrow 37
6.2.4 Private Key Backup 37
6.2.5 Private Key Archival 37
6.2.6 Private Key Transfer Into or From a Cryptographic Module 37
6.2.7 Private Key Storage on Cryptographic Module 38
6.2.8 Method of Activating Private Key 38
6.2.9 Method of Deactivating Private Key 38
6.2.10 Method of Destroying Private Key 38
6.2.11 Cryptographic Module Capabilities 38

6.3 Other Aspects of Key Pair Management 38
6.3.1 Public Key Archival 38
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 38

6.4 Activation Data 39
6.4.1 Activation Data Generation and Installation 39
6.4.2 Activation Data Protection 39
6.4.3 Other Aspects of Activation Data 39

6.5 Computer Security Controls 39
6.5.1 Specific Computer Security Technical Requirements 39
6.5.2 Computer Security Rating 39

6.6 Lifecycle Technical Controls 39
6.6.1 System Development Controls 39
6.6.2 Security Management Controls 40
6.6.3 Lifecycle Security Controls 40

6.7 Network Security Controls 40

6.8 Timestamping 40

7 Certificate, CRL, and OCSP Profiles 41

7.1 Certificate Profile 41
7.1.1 Version Number(s) 41
7.1.2 Certificate Content and Extensions 41
7.1.3 Algorithm Object Identifiers 41
7.1.4 Name Forms 41
7.1.5 Name Constraints 41
7.1.6 Certificate Policy Object Identifier 41
7.1.7 Usage of Policy Constraints Extension 41
7.1.8 Policy Qualifiers Syntax and Semantics 41

7.2 CRL Profile 41
7.2.1 Version Number(s) 41
7.2.2 CRL and CRL Entry Extensions 41

7.3 OCSP Profile 41
7.3.1 Version Number(s) 41
7.3.2 OCSP Extensions 42

8 Compliance Audit and Other Assessments 43

8.1 Frequency and Circumstances of Assessment 43

8.2 Identity/Qualifications of Assessor 43

8.3 Assessor's Relationship to Assessed Entity 43

8.4 Topics Covered by Assessment 43

8.5 Actions Taken as a Result of Deficiency 43

8.6 Communications of Results 43
8.6.1 Self-Audits 43

9 Other Business and Legal Matters 44

9.1 Fees 44
9.1.1 Certificate Issuance or Renewal Fees 44
9.1.2 Certificate Access Fees 44
9.1.3 Revocation or Status Information Access Fees 44
9.1.4 Fees for Other Services 44
9.1.5 Refund Policy 44

9.2 Financial Responsibility 44
9.2.1 Insurance Coverage 44
9.2.2 Other Assets 44
9.2.3 Insurance or Warranty Coverage for End Entities 44

9.3 Confidentiality of Business Information 44
9.3.1 Scope of Confidential Information 44

9.3.2 Information Not Within the Scope of Confidential Information 45
9.3.3 Responsibility to Protect Confidential Information 45

9.4 Privacy of Personal Information 45
9.4.1 Privacy Plan 45
9.4.2 Information Treated as Private 45
9.4.3 Information Not Deemed Private 45
9.4.4 Responsibility to Protect Private Information 45
9.4.5 Notice and Consent to Use Private Information 45
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 45
9.4.7 Other Information Disclosure Circumstances 45

9.5 Intellectual Property rights 45

9.6 Representations and Warranties 46
9.6.1 CA Representations and Warranties 46
9.6.2 RA Representations and Warranties 47
9.6.3 Subscriber Representations and Warranties 47
9.6.4 Relying Party Representations and Warranties 47
9.6.5 Representations and Warranties of Other Participants 48

9.7 Disclaimers of Warranties 48

9.8 Limitations of Liability 48

9.9 Indemnities 48
9.9.1 Indemnification by TrustFactory CA 48
9.9.2 Indemnification by Subscribers 49
9.9.3 Indemnification by Relying Parties 49

9.10 Term and Termination 49
9.10.1 Term 49
9.10.2 Termination 49
9.10.3 Effect of Termination and Survival 49

9.11 Individual Notices and Communications with Participants 49

9.12 Amendments 49
9.12.1 Procedure for Amendment 49
9.12.2 Notification Mechanism and Period 50
9.12.3 Circumstances Under Which OID Must be Changed 50

9.13 Dispute Resolution Provisions 50

9.14 Governing Law 50

9.15 Compliance with Applicable Law 50

9.16 Miscellaneous Provisions 50
9.16.1 Entire Agreement 51
9.16.2 Assignment 51
9.16.3 Severability 51
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 51
9.16.5 Other Provisions 51

Document History

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 Introduction

This Certificate Policy (CP) applies to the certification products and services of TrustFactory PKI. The latest version may be found on the TrustFactory company Repository at https://www.trustfactory.net/repository.

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

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

TrustFactory Certification Authorities (CA) are governed by this CP together with a Certification Practice Statement (CPS) applicable to the Issuing 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. 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 shall be referred to as Issuing CAs).**

1.1 Overview

A CP establishes the requirements and standards imposed on participants within the a PKI hierarchy. The purpose of this CP is to present TrustFactory policies, standards, processes and procedures in managing the hierarchy of TrustFactory 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 System is shown in Figure 1 below:

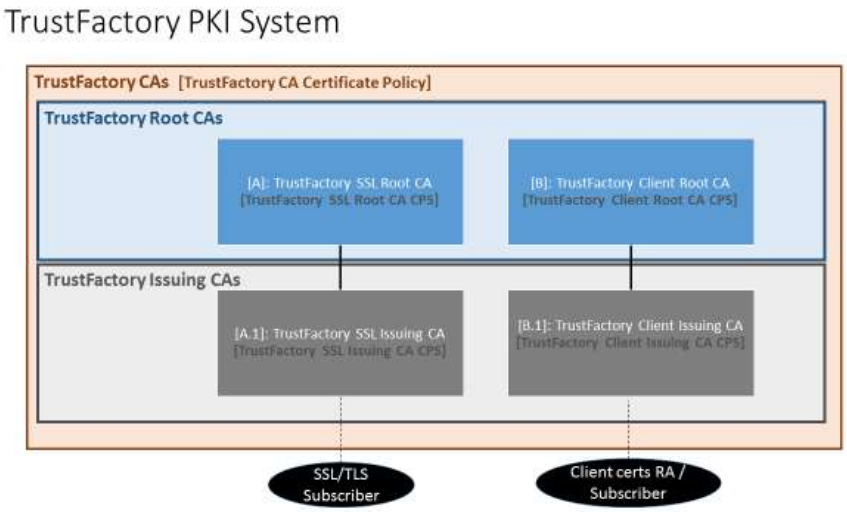

Figure 1: TrustFactory PKI System

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; and
- The TrustFactory Subscriber Agreement
- The TrustFactory Relying Party Agreement

All applicable TrustFactory 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 exact names of the TrustFactory CA Certificates governed by this CP are:

1. TrustFactory SSL Root CA - with serial number 01
2. TrustFactory SSL Issuing CA - with serial number 03
3. TrustFactory Client Root CA - with serial number 02
4. TrustFactory Client Issuing CA - with serial number 04

TrustFactory accepts comments regarding this CP addressed to the address stated in Section 1.5, *Policy Administration.*

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 CP
1.3.6.1.4.1.50318.2.1	TrustFactory SSL Root CA Certificates Practice Statement
1.3.6.1.4.1.50318.2.2	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

1.3 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 creates, signs and issues Issuing CA Certificates.

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

The TrustFactory Policy Authority (PA), is responsible for maintaining this Certificate Policy relating to all Certificates in the TrustFactory PKI hierarchy. Through its Policy Authority, TrustFactory has ultimate control over the lifecycle and management of the TrustFactory Root CAs and any subsequent Subordinate/Issuing CAs. The PA is composed of the TrustFactory General Manager and up to two members appointed by the Directors of the TrustFactory business.

1.3.2 Registration Authorities

An RA is responsible for identifying and authenticating Applicants for Certificates, as well as providing revocation requests for Certificates and requests for re-key, re-issuance and renewal of Certificates. TrustFactory CAs may act as a Registration Authority for Certificates they issue.

Third party entities who are approved by the TrustFactory PA and who enter into an RA Agreement with TrustFactory may operate as an RA and authorize the issuance of Certificates. Third parties must comply with all the requirements of this CP and the terms of their contract. RA's may implement more restrictive 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 of identity and Certificate issuance, a Subscriber is referred to as an *Applicant*.

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 and usage parameters to determine the suitability of the certificate for a particular use.

To verify the validity of a Certificate, Relying Parties must always refer to the applicable Issuing CA revocation information.

1.3.5 Other Participants

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

1.4 Certificate usage

1.4.1 Appropriate Certificate Usage

TrustFactory offers a range of distinct Certificate types. The different Certificate types have differing intended usages and applications. Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Subscribers should appropriately study their requirements for their specific application before applying for a specific Certificate.

The relevant TrustFactory Issuing CA's CPS contains details about the different Certificate types and appropriate uses. 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

1.5.1 Organization Administering the Document

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

TrustFactory Policy Authority
c/o iSolv Technologies
Rosebank Office Park, Block A, 1st floor,
181 Jan Smuts Avenue,
Parktown North
Johannesburg, 2163
South Africa
Tel: +27-11-880 6103
Fax: +27-11-880 6103
Email: info@trustfactory.net

1.5.2 Contact Person

Chairperson - TrustFactory Policy Authority
c/o iSolv Technologies
Rosebank Office Park, Block A, 1st floor,
181 Jan Smuts Avenue,
Parktown North
Johannesburg, 2163
South Africa
Tel: +27-11-880 6103
Fax: +27-11-880 6103
Email: info@trustfactory.net

1.5.3 Person Determining CP 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. The Policy Authority shall approve the CPS for each CA that issues certificates under this policy.

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 Subscribers including the Subscribers and parties relying on Certificates that have been issued under a previous version of the CP.

Meaningful changes to this CP will be evidenced 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's Validity Period.

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

Internet Domain Name System.

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

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

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

Hardware Security Module (HSM): A HSM is type of secure cryptoprocessor targeted at managing digital keys, accelerating cryptoprocesses 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, or there exists a practical technique by which an unauthorized person may discover its value.

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

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a Country's legal system.

Object Identifier (OID): A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

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

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.

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.

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

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

AATL	Adobe Approved Trust List
AES	Advanced Electronic Signature
AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface
ARL	Authority Revocation List (A CRL for Issuing CAs rather than end entities)
AOR	Authorized Organizational Representative
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DNS	Domain Name System
DV	Domain Validation
EIR	Electric Industry Registry
EKU	Extended Key Usage
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ID	Identity document
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LRA	Local Registration Authority
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validation
PKI	Public Key Infrastructure
PA	Policy Authority
RA	Registration Authority
RFC	Request for Comments
SAAA	South African Accreditation Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VAT	Value Added Tax

2 Publication and Repository Responsibilities

2.1 Repositories

TrustFactory CA publishes this CP and any CPS, CA Certificates, Subscriber Agreements, Relying Party agreements, and CRLs in 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 sensitive and/or 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 publishes the current status of issued certificates through CRLs in the Repository or an Online Certificate Status Protocol (OCSP) responder.

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 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 shall annually review and update the Certificate Policy and/or Certification Practice Statement to ensure they comply with the latest version of the Baseline Requirements. 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.

2.4 Access control on repositories

TrustFactory CA shall provide unrestricted read access to its Repositories. Security controls shall be implemented to prevent unauthorized persons from adding, deleting, or modifying repository entries. TrustFactory proves the integrity and authenticity of its public documentation through the use of Digital Signatures applied to PDF documents.

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

Where DNs (Distinguished Names) are used, CNs (Common Names) must respect name space uniqueness and must not be misleading.

3.1.2 Need for Names to be Meaningful

When applicable, TrustFactory CAs shall use distinguished names to identify both the Subject and issuer name of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

TrustFactory CAs shall not issue anonymous or pseudonymous certificates, except in the case of issuing certificates for testing or demonstration where such certificates will be referred to as "test" 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 must ensure that each of its subscribers is identifiable by a unique name. Each X.500 name assigned to a subscriber by a CA (i.e., in that CA's namespace) must identify that subscriber uniquely. When other name forms are used, they too must be allocated such that each name identifies only one subscriber of that CA. Name uniqueness is not violated when multiple certificates are issued to the same entity. For certificates that assert organization names, the name shall be uniquely associated with a specific Authorized Organizational Representative AOR.

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 will validate or verify the Applicant using any legal means of communication or investigation necessary to identify the Legal Entity or individual.

TrustFactory CAs may use the result of a successful Subject DN initial identity validation process to provide alternative products and services that rely on using the same validated information.

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 and Domain Identity

Where an organization identity is inclused 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 and any methods used must be highlighted in the CPS.

For all SSL/TLS Certificates, the Applicant's ownership or control of all requested Domain Name(s) must be verified with methods to achieve this detailed within the CPS.

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.

3.2.2.1 Machine, Device, Department, and Role based Certificate Authentication

TrustFactory CAs must ensure that requests for machine, device, department, or role-based Certificates are authenticated by an RA, acting on behalf of the Issuing CA, that is contractually obligated to the Issuing CA to ensure that machine, device, department, or role-based names relating to the organization and its business are accurate and correct.

3.2.3 Authentication of Individual identity

TrustFactory CAs will issue client end entity certificates as described in the Issuing CA CPS. RAs shall authenticate individuals using criteria, specified in the CPS, that depends upon the type of Client Certificate and level of assurance required.

3.2.3.1 Local Registration Authority Authentication

For enterprise or managed services accounts where a Local Registration Authority (LRA) 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 acting in the capacity of a Local Registration Authority must authenticate individuals affiliated with the organization and issue Certificates based on the Organization Certificate Profile.

3.2.4 Non Verified Subscriber Information

Information that is not verified shall not be included in certificates

3.2.5 Validation of Authority

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall 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 Renewal Requests

Certificate renewal requests must be authenticated.

TrustFactory Issuing CAs permit Certificate renewal prior to the expiry of the Subscriber's existing Certificate. Subscriber identity is established through log in to the Subscriber Management Portal and use of the current signature key, except that identity validation shall be repeated following the same procedures as the initial registration if more than 825 days has lapsed from the time of previous validation.

3.4 Identification and Authentication for Re-key Requests

TrustFactory Root CAs do not support re-key or re-issue.

TrustFactory Issuing CAs 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.

3.4.1 Identification and Authentication for Routine Re-key

For re-key of any subscriber certificate issued under this certificate policy, identity is established through log in to the Subscriber Management Portal 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 must be re-performed and a new Certificate issued with the validated information.

3.4.1.1 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.

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

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

3.5 Identification and Authentication for Revocation Request

All revocation requests must be authenticated by the TrustFactory CA. Revocation requests may be received from the Subscriber (including designated representatives), the administrative contact of the RA or an enterprise Administrator of the LRA.

Revocation requests from Subscribers will be granted if initiated after logging into the Subscriber Management Portal. Revocation requests via email may be granted if the request has been suitably verified.

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, or an RA on behalf of the Subscriber.

TrustFactory CAs may maintain their own blacklists for individuals from whom or entities from which they will 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 shall 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 shall obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement or Terms of Use, which may be electronic.
3. Any additional documentation request 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 a 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 using a multi-factor authentication mechanism.

4.2.2 Approval or Rejection of Certificate Applications

TrustFactory CAs shall reject applications for Certificates where validation of all items cannot be successfully completed.

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

TrustFactory CAs may reject applications including for the following reasons:

- Based on potential brand damage to TrustFactory CA in accepting the application.
- For Certificates from Applicants who have previously been rejected or have previously violated a provision of a Subscriber Agreement.

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 shall ensure that all reasonable methods are used in order to process and evaluate Certificate applications within 30 days of receiving the application.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

TrustFactory Issuing CAs accept certificate issuance requests directly or from RAs approved by the TrustFactory PA. RAs directly operated by the TrustFactory CA or RAs contracted by the TrustFactory CA to perform validation shall ensure that all information sent to the CA is verified and authenticated in a secure manner.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

The Issuing CA shall notify the Subscriber of the issuance of a Certificate using the email information submitted during the enrollment process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

TrustFactory CAs shall inform the Subscriber that s/he may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. To avoid this being an open ended stipulation, TrustFactory CAs may deem a Certificate to be accepted after seven days from receipt 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 sending the Certificate to 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

No stipulation

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

TrustFactory CAs 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 back- up 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 and key usage extensions. Relying Parties should use the information to make a risk assessment 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 defined as the production of a new Certificate that has the same details as a previously issued Certificate and the same Public Key. A TrustFactory CA may renew a Certificate so long as:

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

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.

4.6.2 Who May Request Renewal

A TrustFactory CA may accept a renewal request provided that it is authorized by the original Subscriber through a suitable Certificate lifecycle account challenge response. The CSR used must contain the same Public Key.

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

4.6.3 Processing Certificate Renewal Requests

Renewal requests may be processed using the same process used for initial certificate issuance, except that identity shall be re-validated following the same procedures as the initial registration if 825 days has elapsed since the previous validation.

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.7 Certificate Re-Key / Re-Issue

4.7.1 Circumstances for Certificate Re-Key / Re-Issue

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 / Re-Issue request provided that it is authorized by either the original Subscriber, or an AOR who retains responsibility for the Private Key, and is suitably authenticated through the Subscriber Management Portal. A CSR is mandatory with any new Public Key.

4.7.3 Processing Certificate Re-Key / Re-Issue Requests

A TrustFactory CA may request additional information before processing a re-key or reissue request and re-validates the Subscriber subject to re-verification of any previously validated data. Subscriber authentication through the Subscriber Management Portal is acceptable.

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/ Re-Issued Certificate

As per 4.4.1

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

As per 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.8 Certificate Modification

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

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A certificate shall 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 shall describe specific circumstances for revocation. Whenever a revocation circumstance occurs, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

The CRL itself will then 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 shall accept authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the RA, Subscriber or the AOR of an organization named in the Certificate. TrustFactory CAs may also at their own discretion revoke Certificates

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

4.9.3 Procedure for Revocation Request

Due to the nature of revocation requests and the need for efficiency, TrustFactory CAs and RAs shall provide automated mechanisms for requesting and authenticating revocation requests; for example, through an account which issued the Certificate that is requested to be revoked. RAs may also provide

manual backup processes in the event that automated revocation methods are not possible.

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

Once revoked, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason codes may be included. CRLs may be published immediately or they may be published as defined within the TrustFactory CA's CPS.

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

TrustFactory CAs do not support bulk revocation.

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 decide whether revocation or other appropriate action is warranted based on at least the following criteria:

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

TrustFactory CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests received within 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. Relying Parties will need to consult the CRL or OCSP information for each Certificate in the chain as well as validating that the Certificate chain itself is complete and follows IETF PKIX standards.

4.9.7 CRL Issuance Frequency

TrustFactory CAs that operate online must publish CRLs at least every 24 hours.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the Repository within a commercially reasonable time after generation.

Furthermore, each CRL shall be published no later than the time specified in the *nextUpdate* field of the previously issued CRL for same scope.

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.

For the status of Subscriber Certificates:

- The TrustFactory Issuing CA shall update information provided via an Online Certificate Status

Protocol at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.

For the status of Subordinate CA Certificates:

- The TrustFactory Root CA 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

No stipulation

4.9.12 Special Requirements Related to Key Compromise

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

Where compromise is confirmed all Subscriber Certificates shall be revoked.

4.9.13 Notification of Certificate Revocation to Subscriber

A Subscriber is notified of the revocation of a Certificate using the email information submitted during the enrollment process.

For Issuing CA Certificate revocation, the Policy Authority is notified of the revocation and a notice placed on the Repository.

4.9.14 Circumstances for Suspension

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

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of TrustFactory CA issued certificates is available via a CRL distribution point or an OCSP responder or both.

4.10.2 Service Availability

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

The TrustFactory 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

4.10.4 End of Subscription

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

4.11 Key Escrow and Recovery

4.11.1 Key Escrow and Recovery Policy and Practices

CA Private Keys are never escrowed.

TrustFactory CAs do not offers key escrow services.

4.11.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable

5 Facility, Management, and Operational Controls

This section of the CP outlines the security policy, physical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

TrustFactory asserts that it makes every reasonable effort to ensure that:

- Logical and physical access to CA systems and data is restricted to authorized individuals;
- The continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity.

5.1 Physical Controls

All TrustFactory CA equipment, including cryptographic modules, are protected from theft, loss, physical damage and unauthorized access at all times. TrustFactory CAs 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 CAs ensure that the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs are housed in secure areas with appropriate security barriers and entry controls.

The TrustFactory CA hardware and software are hosted in a high security caged enclosure (the vault) within a data center with physical security and access control procedures that meet industry standards. The vault barriers extend from real floor to real ceiling to prevent unauthorized entry.

The data center is made of concrete and steel construction.

5.1.2 Physical Access

TrustFactory CAs and RAs shall ensure that the facilities used for Certificate lifecycle management are operated in an environment that physically protects the services from compromise through unauthorized access to systems or data. All TrustFactory office entrances and exits are secured and monitored by security personnel, reception staff, or monitoring/control systems

TrustFactory CAs systems operate within secure data centers (vaults) that provide four layers of security to access sensitive hardware. A 24x7 Closed Circuit TV (CCTV) monitoring system as well as digital recording is provided. Only authorized personnel are allowed into the data center, with TrustFactory personnel accompanying any third party that needs access into the vault. Access control is managed via an electronic access control system with biometric access control at the vault entry/exit points. All successful access entry into the vault is logged.

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposures

TrustFactory CAs servers are protected against water leaks. CA systems are located above ground and placed on raised flooring.

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

Media containing private key material shall be handled, packaged, and stored in a manner consistent with stipulations in Section 5.1.2.

5.1.7 Waste Disposal

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

Paper documents and magnetic media containing sensitive or confidential information are securely disposed of by:

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

5.1.8 Off-Site Backup

TrustFactory CAs performs routine backups of critical system data, audit log data, and other essential business information. Critical systems backup media are stored in a physically secure manner at an offsite facility. The back-up facilities and procedures ensure that all essential business information, processes and software can be recovered following a disaster or storage media failure.

Back-up arrangements for individual systems are regularly tested to ensure that they meet the requirements of business continuity plans. Backup media are stored at an offsite location (at a location separate from the Certificate issuance equipment), with physical and procedural controls commensurate to that of the operational facility.

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

Backup and recovery procedures are documented in the TrustFactory operational procedures documents and the business continuity plans.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

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

- PKI Administrator
    - cryptographic key life cycle management functions (generation, revocation and renewal of subscriber certificates)
    - handling of Applicant/Subscriber information
- PKI Operator
    - support in executing the cryptographic key life cycle management procedures (generation, revocation and renewal of certificates)
    - handling of Applicant/Subscriber information
- Security Officer:
    - overall responsibility for administering the CA's information security management system policies and processes
    - viewing of CA system archives and audit logs
    - PKI systems asset management
    - key ceremony: compliance, handling and protection of key materials
- Systems Administrator:
    - installation, configuration and maintenance of the CA server systems
    - viewing and monitoring of CA system archives and audit logs
    - day-to-day operation, backup and recovery of CA systems
    - administration of the server operating systems
- Management:
    - approving access to systems and facilities
    - authorization of tasks
    - overall management and coordination of CA functions

Key Ceremony only roles:

- Crypto-equipment technician (CET)
  - 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.
- HSM Administrator
  - administration of HSM
  - can be a backup/stand-in for the CET
- Shareholder:
  - holder of a key share
- Normal Crypto User:
  - key ceremony role
  - 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

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

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

	ADMIN tasks	SHAREHOLDER tasks	USER tasks
ROOT CAs	2 of 3	3 of 5	1 of 1
ISSUING CAs	2 of 3	2 of 3	1 of 1

5.2.3 Identification and Authentication for Each Role

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

Each role described above is identified and authenticated in a manner to guarantee that the right person has the right role to support the CA.

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 are specifically designated to the trusted roles defined in Section 5.2.1 above and it is not permitted for any one person to serve in more than one operational trusted role at the same time.

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

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

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

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

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

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

5.3.2 Background Check Procedures

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

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

Persons fulfilling Trusted Roles pass a background check, comprising identity verification and criminal record checks. CAs have a process in place to ensure employees undergo security background checks at least every 5 years.

5.3.3 Training Requirements

TrustFactory CAs 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 perform
- Disaster recovery and business continuity procedures

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

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 will be retrained when any significant change to the operations is required.

Refresher training shall be conducted as and when required.

5.3.5 Job Rotation Frequency and Sequence

TrustFactory CAs should ensure that any change in the staff will 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 are subjected to the same security controls, verification and training processes as permanent CA personnel.

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files 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 should 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 includes 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.

5.4.2 Frequency of Processing Log

Audit logs for all TrustFactory CAs are reviewed by the Security Officer on a weekly basis for any evidence of malicious activity and following each important operation.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained for at least seven years.

5.4.4 Protection of Audit Log

The records of events and audit logs are protected in a manner to prevent alteration. Only authorized trusted individuals are able to perform any operations, such as archiving or transfer to backup media, without modifying integrity, authenticity and confidentiality of the data. The records of events are date stamped in a secure manner.

5.4.5 Audit Log Backup Procedures

Audit logs are backed-up in a secure location, under the control of an authorized trusted role, and separated from their component source generation. Audit log backup should be protected to the same degree as originals.

5.4.6 Audit Collection System (Internal vs. External)

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

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

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

Additionally, the CA'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 should archive records with enough detail to establish the validity of a signature and of the proper operation of the CA system. The CPS should state what events shall be archived, but should include the following categories of events:

- CA key lifecycle management events
- CA and Subscriber Certificate lifecycle management events
- Security events

5.5.2 Retention Period for Archive

The TrustFactory CAs SHALL 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

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

5.5.4 Archive Backup Procedures

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

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

5.5.5 Requirements for Time-Stamping of Records

If a timestamping service is used to date the records, it must comply with the requirements defined in Section 6.8. Irrespective of timestamping methods, all logs must have must have data indicating the date and time at which the event occurred.

5.5.6 Archive Collection System (Internal or External)

The archive collection system complies with the security requirements defined in Section 5.3.

5.5.7 Procedures to Obtain and Verify Archive Information

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

Requests to obtain archive information shall be coordinated by people in trusted roles.

5.6 Key Changeover

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

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

TrustFactory handles incident and compromise according to incident response and management procedures in order to minimize the impact of such events.
The incident management procedures include an assessment to determine if the CA or RA system

needs to be rebuilt, if only some Certificates need to be revoked, and/or if a CA hierarchy needs to be declared as Compromised. Management will determine when it is appropriate to invoke the disaster recovery plan.

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

The business continuity plan includes:

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

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

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

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

5.7.3 Entity Private Key Compromise Procedures

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

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

5.7.4 Business Continuity Capabilities After a Disaster

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

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

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

5.8 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.

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

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

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

TrustFactory CAs shall:

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

Cryptographic keying material used by RAs to sign request and authenticate to the CA shall be generated in FIPS 140 Level 3 validated hardware cryptographic modules.

6.1.2 Private Key Delivery to Subscriber

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

TrustFactory CAs that create Private Keys on behalf of Subscribers may do so only when sufficient security is maintained within the key generation process and any onward issuance process to the Subscriber.

If the TrustFactory Issuing CA or any of its designated RAs generates the Private Key on behalf of the Subscriber, then the TrustFactory Issuing CA shall encrypt the Private Key for transport to the Subscriber.

If the Issuing CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

The TrustFactory Issuing CA must maintain a record of the subscriber acknowledgment of receipt of the key.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

The TrustFactory CAs ensure that its Public Keys are delivered to Relying Parties in such a way as to prevent substitution attacks.

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

TrustFactory CA will 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 issued under this policy shall contain RSA or elliptic curve public keys. Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs.

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

Subordinate CA Certificates

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

Subscriber Certificates

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

*** L and N (the bit lengths of modulus p and divisor q, respectively) are described in the Digital Signature Standard, FIPS 186- 4 (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186- 4.pdf).

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

6.1.6 Public Key Parameters Generation and Quality Checking

TrustFactory CAs shall generate Key Pairs in accordance with FIPS 186-2 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 FIPS 186-2.

RSA: The TrustFactory CAs confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent is in the range between $2^{16}+1$ and $2^{256}- 1$. The modulus has the

following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800- 89].

DSA: Although FIPS 800- 57 says that domain parameters may be made available at some accessible site, compliant DSA certificates include all domain parameters. This is to insure maximum interoperability among relying party software. The TrustFactory CAs confirm that the value of the public key has the unique correct representation and range in the field, and that the key has the correct order in the subgroup. [Source: Section 5.3.1, NIST SP 800- 89].

ECC: The TrustFactory CAs confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 56A: Revision 2].

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 v3.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The TrustFactory CAs 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 encrypt their Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic Module Standards and Controls

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

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

TrustFactory Root and Issuing CAs activate Private Keys for cryptographic operations with multi-person control (using CA activation materials) performing duties associated with their trusted roles. The trusted roles permitted to operates the multi-person controls are strongly authenticated using token and PIN code. The CA Private Key activation, use and backup is always protected with multi-person control as follows:

- Root CAs: through 3 of 5 Shareholder control and 2 of 3 HSM Admin control
- Issuing CAs: through 2 of 3 Shareholder control and 2 of 3 HSM Admin control

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

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

Two backups will be created. One backup will be stored at the primary site and one backup at the DR site.

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 Issuing CA.

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

6.2.6 Private Key Transfer Into or From a Cryptographic Module

TrustFactory Root and Issuing CA Private Keys are generated, activated and stored in Hardware Security Modules. Private key transfer into or from a cryptographic module is performed in secure fashion in accordance to manufacturer guidelines for the module.

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

6.2.7 Private Key Storage on Cryptographic Module

TrustFactory CAs store Private Keys on at least a FIPS 140-2 level 3 device.

6.2.8 Method of Activating Private Key

TrustFactory CAs are responsible for activating the Private Key in accordance with the instructions and documentation provided by the manufacturer of the Hardware Security Module. Subscribers are responsible for protecting Private Keys in accordance with the obligations that are presented in the form of a Subscriber Agreement or Terms of Use.

6.2.9 Method of Deactivating Private Key

TrustFactory CAs shall ensure that Hardware Security Modules that have been activated are not left unattended or otherwise available to unauthorized access. When a TrustFactory Root / Issuing CA is no longer operational, its Private Keys are removed from the Hardware Security Module, it is powered down and physically secured.

6.2.10 Method of Destroying Private Key

TrustFactory CA Private Keys are destroyed when they are no longer needed or when the Certificate to which they correspond have expired or are revoked. Destroying Private Keys means that TrustFactory CAs destroy all associated CA secret activation data in such a manner that no information can be used to deduce any part of the Private Key.

TrustFactory CA personnel shall destroy the CA Private Key by deleting and overwriting the data (via HSM re-initialization or zeroization) or physical destruction (with a metal shredder or hammer). Such destruction shall be documented and witnessed.

6.2.11 Cryptographic Module Capabilities

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

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

TrustFactory CAs must archive Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

Root CA	Client - up to 30 years SSL - up to 30 years
Issuing CA	Client - up to 15 years SSL - up to 15 years
Subscriber	Client - up to 2 years SSL - up to 2 years

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.

In no event shall Issuing CAs issue a Certificate with a validity period greater than 825 days whether as initial issue, re-key, reissue or otherwise.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of TrustFactory CA activation data used to activate TrustFactory CA Private Keys shall be made during a key ceremony (Refer to Section 6.1.1). Activation data is generated automatically by the appropriate HSM and stored on smartcards and handed to the shareholder, who is a trusted person. The delivery method maintain the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

TrustFactory CA activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms. TrustFactory CA activation data is stored on smart cards and kept at a secure location inside tamper-evident packaging.

6.4.3 Other Aspects of Activation Data

TrustFactory CA activation data must only be held by personnel in trusted roles.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

The TrustFactory CA PKI components include the following functions:

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

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

6.5.2 Computer Security Rating

No stipulation.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

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

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

6.6.2 Security Management Controls

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

6.6.3 Lifecycle Security Controls

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

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

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

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

6.7 Network Security Controls

TrustFactory CA PKI components implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of security guards, firewalls, intrusion prevention systems, anti-virus software on all workstations and filtering routers. Unused network ports and services are turned off. Any boundary control devices used to protect the network on which PKI equipment are hosted deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 Timestamping

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

All TrustFactory online CA (Issuing CA) components are regularly synchronized with a time service such as an atomic clock or Network Time Protocol (NTP) service. A dedicated authority, such as a timestamping authority, may be used to provide this trusted time. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates; and
- Issuance of Subscriber end entity Certificates.

Electronic or manual procedures may be used to maintain system time.

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.

7.1.3 Algorithm Object Identifiers

No stipulation

7.1.4 Name Forms

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

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.

7.1.5 Name Constraints

TrustFactory CAs may issue Certificates with name constraints where necessary and mark as critical where necessary.

7.1.6 Certificate Policy Object Identifier

The TrustFactory CP and CPS object identifiers are as stated in Section 1.2

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

7.2 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

No stipulation

7.3 OCSP Profile

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

7.3.1 Version Number(s)

TrustFactory CAs shall issue Version 1 OCSP responses.

7.3.2 OCSP Extensions

No stipulation

8 Compliance Audit and Other Assessments

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

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

8.1 Frequency and Circumstances of Assessment

TrustFactory CAs complete a compliance audit to ensure compliance with the AICPA 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 are performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

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

8.3 Assessor's Relationship to Assessed Entity

TrustFactory has chosen an auditor/assessor who is completely independent from the TrustFactory CA. The current Auditor is KPMG.

8.4 Topics Covered by Assessment

The audit meets the requirements of the audit scheme defined in 8.0 above. These requirements may vary as audit schemes are updated. An audit scheme will be applicable to the TrustFactory CA in the year following the adoption of the updated scheme.

8.5 Actions Taken as a Result of Deficiency

TrustFactory CAs follow the same process if presented with a material non-compliance by external auditors and 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.

8.6 Communications of Results

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

8.6.1 Self-Audits

No stipulation

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

TrustFactory charges fees for the issuance, management, renewal, re-key and re-issue of the various Certificate products that it offers. Such fees are provided on the TrustFactory website (www.trustfactory.net) and presented to Subscribers at the time the service is consumed. TrustFactory reserves the right to change its fee structure from time to time without prior notice to Subscribers.

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

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

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

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

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

No stipulation

9.2.3 Insurance or Warranty Coverage for End Entities

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

9.3 Confidentiality of Business Information

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.

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

- Audit logs from CA and RA systems;
- Internal TrustFactory CA operational policy, standards and process documentation and business performance information
- Audit Reports from internal and independent auditors

- All commercial agreements and financial records
- Any TrustFactory information classified as Internal or Confidential

9.3.2 Information Not Within the Scope of Confidential Information

Certificate status information and any information appearing on Certificates themselves are deemed public.

Any TrustFactory documents classified as Public

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

Certificate status information and any Certificate content is deemed not private.

9.4.4 Responsibility to Protect Private Information

TrustFactory CAs PKI participants 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 is to be used in accordance with this CP, the CPS and the Privacy Policy. Consent to use personal information for validation purposes is obtained during the application / enrolment process. TrustFactory CAs include any required consents in the Subscriber Agreement, including permission required for any additional information to be obtained from third parties that may be applicable to the product or service being offered by the TrustFactory CA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

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

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property rights

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

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

copies in trustworthy software.

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

All Applicants and Subscribers grant to TrustFactory and any approved TrustFactory RA a non-exclusive, worldwide, paid-up, royalty-free license to use, copy, modify, publicly display, and distribute any information that is supplied by an Applicant or a Subscriber, by any and all means and through any and all media whether now known or hereafter devised for the purposes contemplated under the TrustFactory Certificate Policy and applicable TrustFactory CA CPS and any Subscriber's Agreement.

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.

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

TrustFactory CAs use this 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 will immediately notify the appropriate RA.

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

- **Right to Use Domain Name or IP Address**: That, at the time of issuance, TrustFactory CA implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's Subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in TrustFactory CA's Certificate Policy and/or Certification Practice Statement (see Section 3.2);
- **Authorization for Certificate:** That, at the time of issuance, TrustFactory CA implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in TrustFactory CA's Certificate Policy and/or Certification Practice Statement (see Section 3.2.5);
- **Accuracy of Information:** That, at the time of issuance, TrustFactory CA implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in TrustFactory CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **No Misleading Information:** That, at the time of issuance, TrustFactory CA implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in TrustFactory CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA implemented a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in TrustFactory CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **Subscriber Agreement:** That, if TrustFactory CA and Subscriber are not Affiliates, the

Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the Baseline Requirements, or, if TrustFactory CA and Subscriber are Affiliates, the Applicant Representative acknowledged and accepted the Terms of Use (see Section 4.5.1);

- **Status:** That TrustFactory CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
- **Revocation:** That TrustFactory CA will revoke the Certificate for any of the reasons specified in its Certificate Policy.

9.6.2 RA Representations and Warranties

RAs warrant that:

- Verification and Issuance processes are in compliance with this CP and the relevant TrustFactory CA CPS;
- All information provided to TrustFactory CA does not contain any misleading or false information; and
- All translated material provided by the RA is accurate.

9.6.3 Subscriber Representations and Warranties

Subscribers and/or Applicants warrant that:

- Subscriber will provide accurate and complete information at all times to TrustFactory CA, both in the Certificate Request and as otherwise requested by TrustFactory CA in connection with issuance of a Certificate;
- Subscribers and/or Applicant shall take all reasonable measures to maintain sole 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;
- 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.

9.6.4 Relying Party Representations and Warranties

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

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

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

- Verify the validity or revocation of the CA Certificate using current revocation status information as indicated to the Relying Party;
- Take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or this CP;

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

Relying Parties must at all times establish that it is reasonable to rely on a Certificate under the circumstances taking into account circumstances such as the specific application context a Certificate is usedin.
Claims, by Relying Parties, of liability for misuse of the certificate on excluded applications will be disallowed and the Relying Party will be notified by email of the disallowance of such claims.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

TO THE EXTENT PERMITTED BY APPLICABLE LAW, TRUSTFACTORY CA DISCLAIM ALL WARRANTIES, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OUTSIDE THE CONTEXT OF THE TRUSTFACTORY WARRANTY POLICY.

TRUSTFACTORY CA DOES NOT WARRANT:

1. THE ACCURACY OF ANY UNVERIFIABLE PIECE OF INFORMATION CONTAINED IN CERTIFICATES EXCEPT AS IT MAY BE STATED IN THE RELEVANT PRODUCT DESCRIPTION,
2. THE ACCURACY, AUTHENTICITY, COMPLETENESS OR FITNESS OF ANY INFORMATION CONTAINED IN, FREE, TEST OR DEMO CERTIFICATES.

9.8 Limitations of Liability

IN NO EVENT SHALL TRUSTFACTORY CA BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA OR OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, RELIANCE UPON, LICENSE, PERFORMANCE OR NON PERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS CP OR THE RELEVANT CA'S CPS.
IN NO EVENT SHALL TRUSTFACTORY CA BE LIABLE FOR ANY ACTS OF GOD, OR OTHER PARTY'S RESPONSIBILITIES, OR ANY LIABILITY INCURRED IF THE FAULT IN THE VERIFIED INFORMATION ON A CERTIFICATE IS DUE TO FRAUD OR 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 THIS 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.

TO THE EXTENT TRUSTFACTORY CA HAS ISSUED AND MANAGED THE CERTIFICATE IN ACCORDANCE WITH THIS CP AND THE RELEVANT CA'S CPS, TRUSTFACTORY CA SHALL NOT BE LIABLE TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY LOSSES SUFFERED AS A RESULT OF USE OR RELIANCE ON SUCH CERTIFICATE. OTHERWISE OUTSIDE OF THE CONTEXT OF THE TRUSTFACTORY WARRANTY POLICY, THE RELEVANT TRUSTFACTORY ISSUING CA'S LIABILITY TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY SUCH LOSSES SHALL IN NO EVENT EXCEED THE COST OF THE CERTIFICATE.

THIS LIABILITY CAP LIMITS DAMAGES RECOVERABLE OUTSIDE OF THE CONTEXT OF THE TRUSTFACTORY WARRANTY POLICY. AMOUNTS PAID UNDER THE WARRANTY POLICY ARE SUBJECT TO THEIR OWN LIABILITY CAPS.

THE LIABILITY (AND/OR LIMITATION THEREOF) OF SUBSCRIBERS SHALL BE AS SET FORTH IN THE APPLICABLE SUBSCRIBER AGREEMENTS.
THE LIABILITY (AND/OR LIMITATION THEREOF) OF ENTERPRISE RAS 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. Following publication of the CP and CPS, changes become applicable 30 days thereafter.

9.10.3 Effect of Termination and Survival

TrustFactory CAs will 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 will 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 will be published at the TrustFactory repository with thirty (30) days' notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

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. The revised CP / CPS is deemed to be accepted 30 days after publication.

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

Before resorting to any dispute resolution mechanism including adjudication or any type of alternative dispute resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) complaining parties agree to notify TrustFactory of the dispute in an effort to seek dispute resolution.

Upon receipt of a dispute notice, TrustFactory convenes a dispute committee that advises TrustFactory management on how to proceed with the dispute. The dispute committee convenes within twenty (20) business days from receipt of a dispute notice. The dispute committee is composed by a counsel, a data protection officer, a member of TrustFactory operational management and a security officer. The counsel or data protection officer chair the meeting. In its resolutions the dispute committee proposes a settlement to the TrustFactory executive management. The TrustFactory executive management may subsequently communicate the proposed settlement to the complaining party.

If the dispute is not resolved within twenty (20) business days after initial notice pursuant to CP, parties submit the dispute to arbitration. The arbitration process will be administered by the International Chamber of Commerce (ICC) South Africa in accordance with the ICC Rules of Conciliation and Arbitration.

For all technology related disputes and disputes related to this CP and a TrustFactory CA CPS the parties accept the arbitration authority of an independent expert agreed to by both parties, within 7 (seven) days of being requested to do so by any party

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of the Republic of South Africa shall govern the enforceability, construction, interpretation, and validity of this CP and of all TrustFactory CA CPSs, irrespective of contract or other choice of law provisions. This choice of law is made to ensure uniform procedures and interpretation for all participants, no matter where they are located.
Each party, including TrustFactory CA partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Gauteng, South Africa.

9.15 Compliance with Applicable Law

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

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The TrustFactory CA will contractually obligate every CA and RA involved with Certificate issuance to comply with this 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 will be interpreted in such manner as to effect the original intention of the parties.

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

TrustFactory may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. TrustFactory's failure to enforce a provision of this 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 Other Provisions

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