

PUBLIC



**TrustFactory SSL
Issuing CA
Certification Practice
Statement**

**31st March 2020
Version: 1.6**



Contents

Contents	2
1.0 Introduction.....	9
1.1 Overview	9
1.2 Document Name and Identification	9
1.2.1 Document Revisions.....	10
1.3 PKI Participants.....	10
1.3.1 TrustFactory Certification Authorities	10
1.3.2 Registration Authorities	11
1.3.3 Subscribers	11
1.3.4 Relying Parties	11
1.3.5 Other Participants	11
1.4 Certificate Usage.....	11
1.4.1 Appropriate certificate usage.....	12
1.4.2 Prohibited Certificate usage	12
1.5 Policy Administration.....	13
1.5.1 Organization Administering the Document.....	13
1.5.2 Contact Person	13
1.5.3 Person Determining CPS Suitability for the Policy	13
1.5.4 CPS Approval Procedures	13
1.6 Definitions and acronyms	13
2.0 Publication and Repository Responsibilities.....	19
2.1 Repositories.....	19
2.2 Publication of Certificate Information.....	19
2.3 Time or Frequency of Publication.....	19
2.4 Access controls on repositories	19
3.0 Identification and Authentication	20
3.1 Naming	20
3.1.1 Types of Names	20
3.1.2 Need for Names to be Meaningful	20
3.1.3 Anonymity or pseudonymity of subscribers	20
3.1.4 Rules for Interpreting Various Name Forms	20
3.1.5 Uniqueness of Names.....	20
3.1.6 Recognition, Authentication, and Role of Trademarks	20
3.2 Initial Identity Validation	20
3.2.1 Method to Prove Possession of Private Key	20
3.2.2 Authentication of Organization Identity & Domain Identity.....	20
3.2.3 Authentication of Individual identity.....	23
3.2.4 Non Verified Subscriber Information.....	24
3.2.5 Validation of Authority	24
3.2.6 Criteria for Interoperation.....	24
3.3 Identification and Authentication for Re-key Requests	24
3.3.1 Identification and Authentication for Routine Re-key	24
3.3.2 Identification and Authentication for Re-key after Revocation	24
3.3.3 Identification and Authentication for Renewal Requests	24
3.3.4 Re-verification and Revalidation of Identity When Certificate Information Changes	25



3.4	Identification and Authentication for Revocation Request	25
4.0	Certificate Lifecycle Operational Requirements	26
4.1	Certificate Application	26
4.1.1	Who Can Submit a Certificate Application	26
4.1.2	Enrollment Process and Responsibilities	26
4.2	Certificate Application Processing	26
4.2.1	Performing Identification and Authentication Functions	26
4.2.2	Approval or Rejection of Certificate Applications.....	27
4.2.3	Time to Process Certificate Applications	27
4.3	Certificate Issuance	27
4.3.1	CA Actions during Certificate Issuance	27
4.3.2	Notifications to Subscriber by the CA of Issuance of Certificate.....	27
4.4	Certificate Acceptance	27
4.4.1	Conduct Constituting Certificate Acceptance	27
4.4.2	Publication of the Certificate by the CA	27
4.4.3	Notification of Certificate Issuance by the CA to Other Entities	28
4.5	Key Pair and Certificate Usage	28
4.5.1	Subscriber Private Key and Certificate Usage.....	28
4.5.2	Relying Party Public Key and Certificate Usage	28
4.6	Certificate Renewal.....	28
4.6.1	Circumstances for Certificate Renewal.....	28
4.6.2	Who May Request Renewal	28
4.6.3	Processing Certificate Renewal Requests	28
4.6.4	Notification of New Certificate Issuance to Subscriber	29
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate	29
4.6.6	Publication of the Renewal Certificate by the CA.....	29
4.6.7	Notification of Certificate Issuance by the CA to Other Entities	29
4.7	Certificate Re-Key	29
4.7.1	Circumstances for Certificate Re-Key	29
4.7.2	Who May Request Certification of a New Public Key	29
4.7.3	Processing Certificate Re-Keying Requests.....	29
4.7.4	Notification of New Certificate Issuance to Subscriber	29
4.7.5	Conduct Constituting Acceptance of a Re-Keyed Certificate	29
4.7.6	Publication of the Re-Keyed Certificate by the CA.....	29
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	29
4.8	Certificate Modification / Re-issue.....	30
4.8.1	Circumstances for Certificate Modification	30
4.8.2	Who May Request Certificate Modification	30
4.8.3	Processing Certificate Modification Requests	30
4.8.4	Notification of New Certificate Issuance to Subscriber	30
4.8.5	Conduct Constituting Acceptance of a Modified Certificate.....	30
4.8.6	Publication of the Modified Certificate by the CA	30
4.8.7	Notification of Certificate Issuance by the CA to Other Entities	30
4.9	Certificate Revocation and Suspension	30
4.9.1	Circumstances for Revocation	30
4.9.1.1	Reasons for Revoking a Subscriber Certificate	30
4.9.1.2	Reasons for Revoking a Subordinate CA Certificate	31
4.9.2	Who Can Request Revocation	31
4.9.3	Procedure for Revocation Request.....	32
4.9.4	Revocation Request Grace Period	32
4.9.5	Time Within Which CA Must Process the Revocation Request.....	32



4.9.6	Revocation Checking Requirements for Relying Parties	32
4.9.7	CRL Issuance Frequency	33
4.9.8	Maximum Latency for CRLs	33
4.9.9	On-Line Revocation Status Checking Availability	33
4.9.10	On-Line Revocation Checking Requirements.....	33
4.9.11	Other Forms of Revocation Advertisements Available	33
4.9.12	Special Requirements Related to Key Compromise.....	33
4.9.13	Circumstances for Suspension.....	33
4.9.14	Who Can Request Suspension	33
4.9.15	Procedure for Suspension Request	33
4.9.16	Limits on Suspension Period.....	33
4.10	Certificate Status Services	34
4.10.1	Operational Characteristics	34
4.10.2	Service Availability.....	34
4.10.3	Operational Features.....	34
4.11	End of Subscription	34
4.12	Key Escrow and Recovery.....	34
4.12.1	Key Escrow and Recovery Policy and Practices.....	34
4.12.2	Session Key Encapsulation and Recovery Policy and Practices	34
5.0	Facility, Management, and Operational Controls	34
5.1	Physical Controls.....	34
5.1.1	Site Location and Construction	34
5.1.2	Physical Access	34
5.1.3	Power and Air Conditioning.....	34
5.1.4	Water Exposures	34
5.1.5	Fire Prevention and Protection.....	34
5.1.6	Media Storage	35
5.1.7	Waste Disposal	35
5.1.8	Off-Site Backup	35
5.2	Procedural Controls	35
5.2.1	Trusted Roles.....	35
5.2.2	Number of Persons Required per Task	35
5.2.3	Identification and Authentication for Each Role	35
5.2.4	Roles Requiring Separation of Duties	35
5.3	Personnel Controls.....	35
5.3.1	Qualifications, Experience, and Clearance Requirements.....	35
5.3.2	Background Check Procedures	35
5.3.3	Training Requirements	35
5.3.4	Retraining Frequency and Requirements	35
5.3.5	Job Rotation Frequency and Sequence	35
5.3.6	Sanctions for Unauthorized Actions	35
5.3.7	Independent Contractor Requirements	35
5.3.8	Documentation Supplied to Personnel.....	35
5.4	Audit Logging Procedures	35
5.4.1	Types of Events Recorded	35
5.4.2	Frequency of Processing Logs.....	36
5.4.3	Retention Period for Audit Log	36
5.4.4	Protection of Audit Log	36
5.4.5	Audit Log Backup Procedures	36
5.4.6	Audit Collection System (Internal vs. External).....	37
5.4.7	Notification to Event-Causing Subject	37
5.4.8	Vulnerability Assessments.....	37



5.5	Records Archival	37
5.5.1	Types of Records Archived	37
5.5.2	Retention Period for Archive	37
5.5.3	Protection of Archive.....	37
5.5.4	Archive Backup Procedures	37
5.5.5	Requirements for Timestamping of Records	37
5.5.6	Archive Collection System (Internal or External)	37
5.5.7	Procedures to Obtain and Verify Archive Information	37
5.6	Key Changeover	37
5.7	Compromise and Disaster Recovery.....	37
5.7.1	Incident and Compromise Handling Procedures	37
5.7.2	Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted	37
5.7.3	Recovery Procedures After Key Compromise.....	37
5.7.4	Business Continuity Capabilities after a Disaster.....	38
5.8	CA or RA Termination	38
6.0	Technical Security Controls	39
6.1	Key Pair Generation and Installation.....	39
6.1.1	Key Pair Generation.....	39
6.1.2	Private Key Delivery to Subscriber.....	39
6.1.3	Public Key Delivery to Certificate Issuer	39
6.1.4	CA Public Key Delivery to Relying Parties	39
6.1.5	Key Sizes	39
6.1.6	Public Key Parameters Generation and Quality Checking	40
6.1.7	Key Usage Purposes	40
6.2	Private Key Protection and Cryptographic Module Engineering Controls	40
6.2.1	Cryptographic Module Standards and Controls	40
6.2.2	Private Key (n out of m) Multi-Person Control.....	40
6.2.3	Private Key Escrow	40
6.2.4	Private Key Backup	40
6.2.5	Private Key Archival	40
6.2.6	Private Key Transfer Into or From a Cryptographic Module	40
6.2.7	Private Key Storage on Cryptographic Module	40
6.2.8	Method of Activating Private Key	40
6.2.9	Method of Deactivating Private Key	40
6.2.10	Method of Destroying Private Key.....	40
6.2.11	Cryptographic Module Capabilities.....	40
6.3	Other Aspects of Key Pair Management.....	41
6.3.1	Public Key Archival	41
6.3.2	Certificate Operational Periods and Key Pair Usage Periods	41
6.4	Activation Data	41
6.4.1	Activation Data Generation and Installation	41
6.4.2	Activation Data Protection	41
6.4.3	Other Aspects of Activation Data	41
6.5	Computer Security Controls	41
6.5.1	Specific Computer Security Technical Requirements	41
6.5.2	Computer Security Rating.....	41
6.6	Lifecycle Technical Controls	41
6.6.1	System Development Controls	41
6.6.2	Security Management Controls	41
6.6.3	Lifecycle Security Controls.....	41
6.7	Network Security Controls	41



6.8	Time Stamping	41
7.0	Certificate, CRL, and OCSP Profiles	43
7.1	Certificate Profile	43
7.1.1	Version Number(s)	43
7.1.2	Certificate Extensions	43
7.1.3	Algorithm Object Identifiers	44
7.1.4	Name Forms	44
7.1.5	Name Constraints	45
7.1.6	Certificate Policy Object Identifier	45
7.1.7	Usage of Policy Constraints Extension	46
7.1.8	Policy Qualifiers Syntax and Semantics	46
7.1.9	Processing Semantics for the Critical Certificate Policies Extension	46
7.2	CRL Profile	46
7.2.1	Version Number(s)	46
7.2.2	CRL and CRL Entry Extensions	47
7.3	OCSP Profile	47
7.3.1	Version Number(s)	47
7.3.2	OCSP Extensions	47
8.0	Compliance Audit and Other Assessments	47
8.1	Frequency and Circumstances of Assessment	47
8.2	Identity/Qualifications of Assessor	47
8.3	Assessor's Relationship to Assessed Entity	47
8.4	Topics Covered by Assessment	48
8.5	Actions Taken as a Result of Deficiency	48
8.6	Communications of Results	48
8.7	Self Audits	48
9.0	Other Business and Legal Matters	48
9.1	Fees	48
9.1.1	Certificate Issuance or Renewal Fees	48
9.1.2	Certificate Access Fees	48
9.1.3	Revocation or Status Information Access Fees	48
9.1.4	Fees for Other Services	48
9.1.5	Refund Policy	48
9.2	Financial Responsibility	48
9.2.1	Insurance Coverage	48
9.2.2	Other Assets	48
9.2.3	Insurance or Warranty Coverage for End Entities	48
9.3	Confidentiality of Business Information	48
9.3.1	Scope of Confidential Information	48
9.3.2	Information Not Within the Scope of Confidential Information	48
9.3.3	Responsibility to Protect Confidential Information	48
9.4	Privacy of Personal Information	49
9.4.1	Privacy Plan	49
9.4.2	Information Treated as Private	49
9.4.3	Information Not Deemed Private	49
9.4.4	Responsibility to Protect Private Information	49
9.4.5	Notice and Consent to Use Private Information	49
9.4.6	Disclosure Pursuant to Judicial or Administrative Process	49



9.4.7	Other Information Disclosure Circumstances	49
9.5	Intellectual Property rights	49
9.6	Representations and Warranties.....	49
9.6.1	CA Representations and Warranties	49
9.6.2	RA Representations and Warranties	49
9.6.3	Subscriber Representations and Warranties	49
9.6.4	Relying Party Representations and Warranties	49
9.6.5	Representations and Warranties of Other Participants.....	49
9.7	Disclaimers of Warranties	49
9.8	Limitations of Liability.....	49
9.9	Indemnities	49
9.10	Term and Termination	50
9.10.1	Term 50	
9.10.2	Termination	50
9.10.3	Effect of Termination and Survival	50
9.11	Individual Notices and Communications with Participants.....	50
9.12	Amendments	50
9.12.1	Procedure for Amendment	50
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	50
9.16.2	Assignment.....	50
9.16.3	Severability.....	50
9.16.4	Enforcement (Attorney's Fees and Waiver of Rights).....	50
9.17	Other Provisions	50
Annexure A:	SSL CA Certificate Profiles.....	51
	TrustFactory SSL Issuing CA – Certificate Profile	51
	DOMAINPASS Certificate Profile.....	52
	ORGANISATIONPASS Certificate Profile.....	53



References and Acknowledgements

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



1.0 Introduction

This Certification Practice Statement (CPS) applies to the products and services of TrustFactory SSL Issuing CA. Primarily this pertains to the issuance and lifecycle management of Certificates including validity checking services. The latest version may be found on the TrustFactory Repository at <https://www.trustfactory.net/repository>.

A CPS highlights the *"procedures under which a Certificate is issued to a particular community and/or class of application with common security requirements"*. This CPS aims to adhere to the content and structure guidance provided in Internet Engineering Task Force (IETF) RFC 3647, dated November 2003. Where certain sections or topics of the RFC do not apply or requirements not defined then the term 'No stipulation' is used.

TrustFactory SSL Issuing CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at <http://www.cabforum.org>. In the event of any inconsistency between this document and the Baseline Requirements, the Baseline Requirements take precedence over this document.

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

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

1.1 Overview

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

- **TrustFactory SSL Issuing CA**

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

The Certificate subject names addressed in this CPS are the following:

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

1.2 Document Name and Identification

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

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

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

1.3.6.1.4.1.50318.1	TrustFactory CA CP
1.3.6.1.4.1. 50318.2.1	TrustFactory SSL Root CA Certificates Practice Statement
1.3.6.1.4.1. 50318.2.3	TrustFactory SSL Issuing CA Certificates Practice Statement



1.2.1 Document Revisions

Version	Description	Date
1.0	Initial for review	6 October 2017
1.1	Error corrections Added certificate serial numbers and certificate profiles.	7 December 2017
1.2	Updates to Section 9.1 Fees Other minor corrections	15 December 2017
1.3	Key changes as follows <ul style="list-style-type: none">Align to CAB Forum domain validation requirements: 3.2.2TrustFactory does not validate OU field: 3.2.4Removed revocation request via email: 3.5Provision to reuse validated documents: 4.2.1, 4.6.3 and 4.7.3Notification of the status of certificate: 4.3.2TrustFactory does not provide subscriber key management services: 6.1Added Product Certificate Profiles: 10.2 and 10.3 Other minor corrections to improve clarity, understanding and remove duplications.	8 August 2018
1.4	Change to rectify typographical error in URL for CRL distribution points (sections 2.2, 4.10.1, 10.2 and 10.3)	13 September 2018
1.5	Updates to incorporate latest CAB Forum changes on revocation requirements, and minor corrections and clarifications.	21 November 2018
1.6	Added further explanations or clarifications relating to some procedures (Sections: 1.3.2, 1.5.2, 2.2, 2.3, 3.2.2.4, 3.2.2.8, 4.2.1, 4.4.2, 4.9.9, 7.1.4) Updated to incorporate further details as required by Mozilla Root Store Policy. Removed use of “no stipulation”. Aligned subsection headings to RFC3647 & CAB Forum Baseline Requirements	31 March 2020

1.3 PKI Participants

1.3.1 TrustFactory Certification Authorities

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

- TrustFactory SSL Root Certificate Authority
 - TrustFactory SSL Issuing Certificate Authority
 - DomainPass Certificate
 - OrganizationPass Certificate

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



1.3.2 Registration Authorities

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

TrustFactory SSL Issuing CA does not use External RAs for SSL certificates

An RA will be responsible for:

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

..

1.3.3 Subscribers

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

DNS Names should be listed in the subjectAltName extension of the following Certificate types:

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

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

- **OrganizationPass Certificates**
- **OrganizationPass Premium Certificates**
- **OrganizationPass Wildcard Certificates**

1.3.4 Relying Parties

A Relying Party is a person, entity, or organization that relies on or uses the TrustFactory SSL Issuing CA Certificate and/or any other information provided in the TrustFactory repository to verify the identity and public key of a Subscriber. A Relying Party may use information in the certificate to determine the suitability of the certificate for a particular use.

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

1.3.5 Other Participants

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

1.4 Certificate Usage



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

1.4.1 Appropriate certificate usage

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

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

- **TrustFactory DomainPass Certificates**

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

The assurance provided is as follows:

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

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

- **TrustFactory OrganizationPass Certificates**

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

The assurance provided is as follows:

- Applicant has demonstrated control of the FQDN that is the Subject of the certificate.
- Applicant organization is a registered company
- Applicant is an authorized representative of the organization

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

- **DomainPass or OrganizationPass Premium Certificates**

Both DomainPass and OrganizationPass Certificates are available as Premium certificates. The specified level domain is vetted and the certificate may be used for upto 100 sub-domains that contain the specified vetted level domain.

- **DomainPass or OrganizationPass Wildcard Certificates**

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

1.4.2 Prohibited Certificate usage

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

Any usage of the Certificate inconsistent with these extensions is not authorized and shall be deemed prohibited usage. Certificates are not authorized for use for any transactions above the designated reliance limits that have been indicated in the TrustFactory Warranty Policy.

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

Certificates issued under this CPS may not be used:

- for any application requiring fail safe performance such as:
 - the operation of nuclear power facilities,



- air traffic control systems,
 - aircraft navigation systems,
 - weapons control systems, and
 - any other system whose failure could lead to injury, death or environmental damage;
- where prohibited by law.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Any enquiry associated with this CPS should be addressed to:

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

1.5.2 Contact Person

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

Subscribers, Relying Parties, Application Software Suppliers, and other third parties can report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, through the “Report Abuse” link on the TrustFactory website at www.trustfactory.net. This opens an email client that sends an email to abuse@trustfactory.net

1.5.3 Person Determining CPS Suitability for the Policy

The TrustFactory Policy Authority determines the suitability and applicability of this CPS and the conformance of this CPS to the TrustFactory CP based on the results and recommendations received from a Qualified Auditor.

1.5.4 CPS Approval Procedures

The TrustFactory Policy Authority reviews and approves any changes to this CPS. The updated CPS is reviewed against the CP in order to check for consistency. CP changes are also added on as needed basis. Upon approval of a CPS update by the Policy Authority, the new CPS is published in the TrustFactory SSL Issuing CA Repository at <https://www.trustfactory.net/repository>.

The updated version is binding upon all Subscribers, for all Certificates that have been issued or are to be issued, including the Subscribers and parties relying on Certificates that have been issued under a previous version of the CPS.

1.6 Definitions and acronyms

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



the initial message has been altered since the transformation was made.

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

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

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

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

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

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

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

Expiry Date: The “notAfter” date in a Certificate that defines the end of a Certificate’s Validity Period.

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

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

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

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

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

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

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

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

Individual: A natural person.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Jurisdiction of Incorporation: In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization’s legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context



of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Key Compromise: A Private Key is said to be Compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the



form of a CRL or an OCSP response.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

AATL	Adobe Approved Trust List
AES	Advanced Electronic Signature
AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface
BR	CA/B Forum Baseline Requirements
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As



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



2.0 Publication and Repository Responsibilities

2.1 Repositories

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

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

2.2 Publication of Certificate Information

TrustFactory SSL Issuing CA publishes its CP, CPS, Subscriber Agreements, and Relying Party agreements at <https://www.trustfactory.net/repository>

Section 4.2 of this CPS states the Issuing CA's policy or practice on processing CAA Records for Fully Qualified Domain Names.

CRLs are published in online repositories. The CRLs contain entries for all revoked unexpired Certificates with a validity period that depends on Certificate type and/or position of the Certificate within the Certificate chain.

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

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

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

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

The specific test URLs are:

- VALID: <https://valid.trustfactory.net>
- EXPIRED: <https://expired.trustfactory.net>
- REVOKED: <https://revoked.trustfactory.net>

2.3 Time or Frequency of Publication

The TrustFactory PA will annually review this CPS and may make revisions and updates to policies as required by changes in the Requirements, standards, laws and regulations or other circumstances. Any updates become binding for all Certificates that have been issued or are to be issued upon the date of the publication of the updated version of this CPS.

New or modified versions of the CP, this CPS, Subscriber Agreements, or Relying Party agreements are published within ten days after being digitally signed by the TrustFactory Policy Authority.

In order to reference that the annual review of this CPS has taken place, TrustFactory will increment the version number and add a dated change log entry, even if no other changes are made to the document.

2.4 Access controls on repositories

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

Access control policies are implemented to prevent unauthorized persons from adding, deleting, or modifying repository entries. TrustFactory ensures that the integrity and authenticity of its public



documentation is maintained by digitally signing the Adobe PDF format of the documents.

3.0 Identification and Authentication

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

3.1 Naming

3.1.1 Types of Names

TrustFactory SSL Issuing CA Certificates are issued with subject DNs (Distinguished Names) which meet the requirements of X.500 naming. Common Names (CNs) respect name space uniqueness and are not misleading.

The common name will be the name associated with the Subscriber to which the Subscriber Certificate is to be issued.

3.1.2 Need for Names to be Meaningful

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

3.1.3 Anonymity or pseudonymity of subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

TrustFactory SSL Issuing CA enforces the uniqueness of each Subject name in a Certificate Authority as follows:

- The combination of the Common Name and all the attributes of the Distinguished Name (DN), together with the certificate serial number provides a unique electronic identity for the Subscriber.

3.1.6 Recognition, Authentication, and Role of Trademarks

TrustFactory SSL Issuing CA may not use registered trademarks that infringe on the intellectual property rights of a third party, when assigning the distinguished names to Subscribers. TrustFactory SSL Issuing CA does not verify if the Applicant has the right to use a requested registered trademark in a certificate.

3.2 Initial Identity Validation

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

3.2.1 Method to Prove Possession of Private Key

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

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

3.2.2 Authentication of Organization Identity & Domain Identity

3.2.2.1 Validation of Organization Identity

For all Certificates that include an organization identity, Applicants are required to provide the organization's registered name and registered or trading address. TrustFactory will verify the identity and



address of the organization and that the address is the Applicant's address of existence or operation using one of the following:

- A government agency in the jurisdiction of the Applicant, or a superior governing governmental agency if the Applicant claims they are a government agency themselves;
- A Reliable Data Source that has been approved by TrustFactory PA as being reasonably accurate and reliable;
- An attestation letter confirming that Subject Identity Information is correct, written by a Notary Public, Registered Chartered Accountant, or other reliable third party customarily relied upon for such information;
- An independent verification agency that operates in the jurisdiction in which the company is registered; or
- A site visit by the RA, or a third party who is acting as an agent for TrustFactory CA
-
- TrustFactory may utilize a Delegated Third Party (including recognized verification agencies) to perform any of the verification activities above.

3.2.2.2 Use of Tradename or DBA name

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

- Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
- A Reliable Data Source has been approved by TrustFactory PA as being reasonably accurate and reliable;
- Communication with a government agency responsible for the management of such DBAs or tradenames;
- An Attestation Letter accompanied by documentary support; or
- A utility bill, bank statement, credit card statement, government-issued tax document, not older than 3 months, that states the DBA name.

3.2.2.3. Verification of Country

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

3.2.2.4 Validation of Domain Authorization or Control

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

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

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

3.2.2.4.1 Validating the Applicant as a Domain Contact

- This method is not permitted.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

TrustFactory confirms the applicants control over the requested FQDN by sending a Random Value



(contained in a verification link) via email only, and then receiving a confirming response utilizing the Random Value (verification link). This verification email is sent to the Domain Name Registrant as obtained from the WHOIS record for the domain. TrustFactory uses an HTTPS connection to send an automated query to a third party WHOIS proxy.

- Domain Contact via Fax, SMS, or Postal Mail is not permitted.

3.2.2.4.3 Phone Contact with Domain Contact

- This method is not permitted.

3.2.2.4.4 Constructed Email to Domain Contact

In certain cases the Domain Name Registrant's email may not be publically available. In this case, TrustFactory confirms the Applicant's control over the FQDN by sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name. This email includes a Random Value (contained in a verification link), and TrustFactory must receive a confirming response utilizing the Random Value (verification link).

3.2.2.4.5 Domain Authorization Document

- This method is not permitted.

3.2.2.4.6 Agreed-Upon Change to Website

Confirming the Applicant's control over the FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

- The presence of Required Website Content contained in the content of a file. The entire Required Website Content must not appear in the request used to retrieve the file or web page, or
- The presence of the Request Token or Random Value contained in the content of a file where the Request Token or Random Value must not appear in the request.

Once the FQDN has been validated using this method, TrustFactory CA may also issue Wildcard Certificates for other domain names that end with all the labels of the validated FQDN.

3.2.2.4.7 DNS Change

- This method is not permitted.

3.2.2.4.8 IP Address

- This method is not permitted.

3.2.2.4.9 Test Certificate

- This method is not permitted.

3.2.2.4.10. TLS Using a Random Number

- This method is not permitted.

3.2.2.4.11 Any Other Method

- This method is not permitted.

3.2.2.4.12 Validating Applicant as a Domain Contact

- This method is not permitted.

3.2.2.4.13 Email to DNS CAA Contact

- This method is not permitted.

3.2.2.4.14 Email to DNS TXT Contact

- This method is not permitted.

3.2.2.4.15 Phone Contact with Domain Contact

- This method is not permitted.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

- This method is not permitted.

3.2.2.5. Authentication for an IP Address

- Not applicable. TrustFactory does not permit listing IP Addresses in a Certificate

3.2.2.6. Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS- ID, the TrustFactory SSL Issuing CA determines if the wildcard character occurs in the first label position to the left of a “registry- controlled” label or “public suffix” (e.g. “.com”).

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

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

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

3.2.2.7 Data Source Accuracy

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

TrustFactory CA consults the following Reliable Data Source lists:

- the WHOIS records where applicable
- the <http://publicsuffix.org/> “public suffix list” / ICANN DOMAINS
- Registrar of Companies database where applicable, or equivalent companies register managed by a responsible public authority
- Dun & Bradstreet DUNS numbers

3.2.2.8 CAA Records

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

TrustFactory’s CAA domains: trustfactory.net

3.2.3 Authentication of Individual identity

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



certificate.

3.2.4 Non Verified Subscriber Information

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

3.2.5 Validation of Authority

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

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

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

3.2.6 Criteria for Interoperation

Not applicable. TrustFactory SSL Issuing CA has not established any cross-certificates.

3.3 Identification and Authentication for Re-key Requests

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

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

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

3.3.1 Identification and Authentication for Routine Re-key

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

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

3.3.2 Identification and Authentication for Re-key after Revocation

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

3.3.3 Identification and Authentication for Renewal Requests

Certificate renewal requests will be authenticated.

TrustFactory SSL Issuing CA permits Certificate renewal prior to the expiry of the Subscriber's existing Certificate. Subscriber identity is established through log in to the Subscriber Management Portal and Certificate renewal request submitted through the Portal. The CSR of the current Certificate is used for the renewed Certificate.



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

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

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

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

3.4 Identification and Authentication for Revocation Request

TrustFactory SSL Issuing CA will accept revocation requests from:

1. The Subscriber, requested via the Subscriber Management Portal (login to the portal is acceptable authentication of the subscriber)
2. The TrustFactory operations team, after it is approved by the CA Administrator

Revocation requests are granted after they are authenticated by the TrustFactory RA.



4.0 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Any applicant who is appropriately authorized, and not included in blacklist, may submit an application for a certificate.

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

4.1.2 Enrollment Process and Responsibilities

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

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

After successful verification, the enrolment process includes the following steps (but the sequence depends on the type of certificate):

- Agreeing to a Subscriber Agreement or other applicable terms and conditions; and paying any applicable fees;
- Submit a CSR from the Subscriber to the TrustFactory SSL Issuing CA;
- The TrustFactory SSL Issuing CA will validate and sign the Subscriber CSR and certificate data submitted; and
- Issue the Subscriber Certificate.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Applicant information must include, but not be limited to, at least one FQDN to be included in the Certificate's SubjectAltName extension. Any other information to be included in the Certificate must be supported with additional documents to enable TrustFactory validation specialists to verify the information, as set forth in Section 3.2. Domain verification for SSL/TLS certificates will be performed by the TrustFactory SSL Issuing CA.

TrustFactory checks the CAA records for each FQDN in the certificate request. If CAA records exist, then TrustFactory will only issue certificates if the domain name *trustfactory.net* is listed in the "issue" and "issuewild" records. If CAA records do not exist then TrustFactory may issue the certificate.

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

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

TrustFactory may use the documents and data provided in Section 3.2 to verify certificate information, and may reuse previous validations themselves, provided that the data or document was obtained no more than 825 days prior to issuing the Certificate.

The TrustFactory SSL Issuing CA checks for High Risk Certificate Requests and will not issue new or



replacement Certificates to an entity if it is deemed High Risk.

4.2.2 Approval or Rejection of Certificate Applications

Assuming all verification steps can be completed successfully following the procedures in this CPS then TrustFactory SSL Issuing CA will generally approve the Certificate Request.

TrustFactory SSL Issuing CA reserves the right to reject applications including for the following reasons:

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

Within 30 days after ICANN has approved a new gTLD for operation, TrustFactory SSL Issuing CA will stop issuing Certificates containing a new gTLD under consideration by ICANN unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name.

Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], TrustFactory SSL Issuing CA will revoke each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name

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

4.2.3 Time to Process Certificate Applications

TrustFactory SSL Issuing CA will ensure that all reasonable methods are used in order to evaluate and process Certificate applications within 30 working days. Where issues outside of the control of TrustFactory SSL Issuing CA occur, TrustFactory SSL Issuing CA will strive to keep the Applicant duly informed.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Notification of the status of certificate issuance is available to the Subscriber on the Subscriber Management Portal. TrustFactory SSL Issuing CA will notify the Subscriber of the issuance of a Certificate at an email address which was supplied by the Subscriber during the enrollment process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

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



4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No further notification to other entities is required.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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

The Subscriber shall use its private key and the Certificate in strict compliance with this CPS. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding Certificate.

4.5.2 Relying Party Public Key and Certificate Usage

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

TrustFactory SSL Issuing CA provides a Relying Party agreement to Subscribers, the content of which should be presented to the Relying Party. Relying Parties should perform a risk assessment to ensure that their reliance on a Certificate is appropriate. Relying Parties must assess:

1. The appropriateness of the use of a Certificate for any given purpose and that it is not prohibited or otherwise restricted by this CPS.
2. That the certificate is being used in accordance with the basic constraints, key usage and extended key usage extensions included in the certificate
3. The revocation status of the certificate and all the CAs in the chain that issued the certificate.

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

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

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

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

The original Certificate will be revoked after renewed certificate is issued.

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

4.6.2 Who May Request Renewal

TrustFactory SSL Issuing CA may accept a renewal request from the Subscriber provided that the renewal request is submitted and properly authenticated via login to the Subscriber Management Portal. A renewal request may be accepted from an AOR who retains responsibility for the Private Key on behalf of a Subscriber.

4.6.3 Processing Certificate Renewal Requests

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

TrustFactory will reuse previously validated documents, if they are still considered valid, to process the



renewal request.

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

Subscribers may request routine re-key.

TrustFactory SSL Issuing CA may re-key a Certificate under the following criteria:

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

The original Certificate will be revoked after re-keyed certificate is issued.

4.7.2 Who May Request Certification of a New Public Key

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

4.7.3 Processing Certificate Re-Keying Requests

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

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

4.7.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3



4.8 Certificate Modification / Re-issue

4.8.1 Circumstances for Certificate Modification

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

- The original Certificate has not been revoked;
- The Public Key from the original Certificate has not been blacklisted for any reason;
- The Subject details remain the same; and
- Only SAN domain field modifications are submitted in the modification request.

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

4.8.2 Who May Request Certificate Modification

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

4.8.3 Processing Certificate Modification Requests

TrustFactory SSL Issuing CA do not allow changes to certificate subject details during modification/re-issue. In the case of a modification/re-issue, authentication through the Subscriber Management Portal is acceptable. Domain validation is performed on any newly added SAN domains.

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

4.8.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

As per 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

As per 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

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

1. The Subscriber requests through the Subscriber Management Portal that TrustFactory SSL Issuing CA revoke the Certificate;
2. The Subscriber notifies TrustFactory SSL Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. TrustFactory CA operations obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
4. TrustFactory CA operations obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name in the Certificate should not be relied upon.

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

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;



2. TrustFactory CA operations obtains evidence that the Certificate was misused;
3. TrustFactory CA operations is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. TrustFactory CA operations is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. TrustFactory CA operations is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. TrustFactory CA operations is made aware of a material change in the information contained in the Certificate;
7. TrustFactory CA operations is made aware that the Certificate was not issued in accordance with the Baseline Requirements or the CA's Certificate Policy or Certification Practice Statement;
8. TrustFactory CA operations determines or is made aware that any of the information appearing in the Certificate is inaccurate;
9. TrustFactory SSL Issuing CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by the TrustFactory SSL Issuing CA's Certificate Policy and/or Certification Practice Statement; or
11. The TrustFactory CA operations is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see <http://wiki.debian.org/SSLkeys>), or if there is clear evidence that the specific method used to generate the Private Key was flawed.
12. TrustFactory CA operations receives a certified copy of the subscribers death certificate
13. TrustFactory CA operations receives documentation that a subscriber that is a legal person has been wound up or registered or has ceased to exist (i.e. organization)

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

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

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

Not applicable.

4.9.2 Who Can Request Revocation

TrustFactory SSL Issuing CA will accept revocation requests submitted via login to the Subscriber Management Portal. A revocation request may be accepted from an organization administrator who retains



responsibility for the Private Key on behalf of a Subscriber, or an affiliated organization named in the Certificate. TrustFactory SSL Issuing CA may also at its own discretion revoke Certificates.

Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports, through the “Report Abuse” link on the TrustFactory website at www.trustfactory.net. [This opens an email client that sends an email to abuse@trustfactory.net](mailto:abuse@trustfactory.net). The individual reporting the certificate problem must provide their identity and contact details as well as the reasonable cause to revoke the certificate.

4.9.3 Procedure for Revocation Request

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

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

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

Once revoked, the serial number of the Certificate and the date and time will be added to the appropriate CRL. CRL reason codes may be included. CRLs are published according to this CPS.

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

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which CA Must Process the Revocation Request

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

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

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

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

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

4.9.6 Revocation Checking Requirements for Relying Parties



Prior to relying upon a Certificate, Relying Parties must validate the suitability of the Certificate to the purpose intended and ensure the Certificate is valid. Relying Parties will need to consult the CRL or OCSP information for each Certificate in the chain as well as validating that the Certificate chain itself is complete and follows IETF PKIX standards.

4.9.7 CRL Issuance Frequency

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

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-Line Revocation Status Checking Availability

OCSP responses conform to RFC6960 and RFC5019.

OCSP responses

are signed by an OCSP Responder whose Certificate is signed by the TrustFactory SSL Issuing CA that issued the Certificate whose revocation status is being checked. In this case, the OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-Line Revocation Checking Requirements

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

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

The SSL Issuing CA does not sign error messages when returned in response to certificate status requests.

TrustFactory SSL Issuing CA supports an OCSP capability using the GET method for Certificates.

4.9.11 Other Forms of Revocation Advertisements Available

No requirements specified.

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

4.9.12 Special Requirements Related to Key Compromise

In the event of compromise of a TrustFactory SSL Issuing CA Private Key used to sign Subscriber Certificates, TrustFactory operations will as soon as practically possible inform the Subscriber that the private key may have been Compromised. This includes cases where TrustFactory operations at its own discretion decides that evidence suggests a possible Key Compromise has taken place.

Where Key Compromise is not disputed, TrustFactory SSL Root CA will revoke Issuing CA Certificates within 24 hours and publish the updated CRL within 24 hours of creation.

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

Not applicable. Certificate suspension is not supported and not permitted

4.9.15 Procedure for Suspension Request

Not applicable. Certificate suspension is not supported and not permitted

4.9.16 Limits on Suspension Period

Not applicable. Certificate suspension is not supported and not permitted



4.10 Certificate Status Services

4.10.1 Operational Characteristics

TrustFactory SSL Issuing CA provides a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both. These services are presented to Relying Parties within the Certificate and the URLs to access the CRL and OCSP are provided in Section 2.2 of this CPS.

1.

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

CRLs are signed by the TrustFactory SSL Issuing CA Private Key.

4.10.2 Service Availability

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

The TrustFactory CA maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report (submitted via the Report Abuse link on the TrustFactory website), and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Operational Features

No requirements specified

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

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

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

5.0 Not applicable Facility, Management, and Operational Controls

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

5.1 Physical Controls

5.1.1 Site Location and Construction

Controls are as defined in the TrustFactory CP.

5.1.2 Physical Access

Controls are as defined in the TrustFactory CP.

5.1.3 Power and Air Conditioning

Controls are as defined in the TrustFactory CP.

5.1.4 Water Exposures

Controls are as defined in the TrustFactory CP.

5.1.5 Fire Prevention and Protection



Controls are as defined in the TrustFactory CP.

5.1.6 Media Storage

Controls are as defined in the TrustFactory CP.

5.1.7 Waste Disposal

Controls are as defined in the TrustFactory CP.

5.1.8 Off-Site Backup

Controls are as defined in the TrustFactory CP.

5.2 Procedural Controls

5.2.1 Trusted Roles

Controls are as defined in the TrustFactory CP

5.2.2 Number of Persons Required per Task

Controls are as defined in the TrustFactory CP

5.2.3 Identification and Authentication for Each Role

Controls are as defined in the TrustFactory CP.

5.2.4 Roles Requiring Separation of Duties

Controls are as defined in the TrustFactory CP

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Controls are as defined in the TrustFactory CP.

5.3.2 Background Check Procedures

Controls are as defined in the TrustFactory CP.

5.3.3 Training Requirements

Controls are as defined in the TrustFactory CP.

5.3.4 Retraining Frequency and Requirements

Controls are as defined in the TrustFactory CP.

5.3.5 Job Rotation Frequency and Sequence

Controls are as defined in the TrustFactory CP.

5.3.6 Sanctions for Unauthorized Actions

Controls are as defined in the TrustFactory CP.

5.3.7 Independent Contractor Requirements

Controls are as defined in the TrustFactory CP.

5.3.8 Documentation Supplied to Personnel

Controls are as defined in the TrustFactory CP.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

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

The TrustFactory SSL Issuing CA records at least the following events:



1. CA key lifecycle management events, including:
 - a. Key generation, backup, storage, recovery, archival, and destruction;
 - Withdrawal of keying material from service;
 - Identity of the entity authorizing a key management operation,
 - Identity of the entity handling any keying material (such as key components or keys stored in portable devices or media);
 - Compromise of a private key.
 - b. Cryptographic device lifecycle management events:
 - device receipt and installation;
 - placing into or removing a device from storage;
 - device activation and usage;
 - device change in state of use.
2. CA and Subscriber Certificate lifecycle management events, including:
 - a. Certificate requests, renewal, and re-key requests, and revocation;
 - b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
 - c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
 - d. Name of submitting RA,
 - e. Acceptance and rejection of certificate requests;
 - f. Issuance of Certificates;
 - g. The subscriber's acceptance of the Subscriber Agreement; and
 - h. Where required under privacy legislation, the Subscriber's consent to allow the TrustFactory to keep records containing personal data, pass this information to specified third parties, and publication of certificates.
 - i. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
 - a. Successful and unsuccessful PKI system access attempts;
 - b. PKI and security system actions performed;
 - c. Security profile changes;
 - d. System crashes, hardware failures, and other anomalies;
 - e. Firewall and router activities; and
 - f. Entries to and exits from the CA facility.

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

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

5.4.2 Frequency of Processing Logs

Audit logs are reviewed as follows:

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

Unauthorized or suspicious activity detected during the reviews is investigated

5.4.3 Retention Period for Audit Log

Controls are as defined in the TrustFactory CP

5.4.4 Protection of Audit Log

Controls are as defined in the TrustFactory CP

5.4.5 Audit Log Backup Procedures

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



a month they are backed up to tape and taken to a vault for storage.

5.4.6 Audit Collection System (Internal vs. External)

Controls are as defined in the TrustFactory CP.

5.4.7 Notification to Event-Causing Subject

No requirements specified

5.4.8 Vulnerability Assessments

1. Controls are as defined in the TrustFactory CP

5.5 Records Archival

5.5.1 Types of Records Archived

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

5.5.2 Retention Period for Archive

Controls as defined in the TrustFactory CP.

5.5.3 Protection of Archive

Controls as defined in the TrustFactory CP

5.5.4 Archive Backup Procedures

Controls as defined in the TrustFactory CP.

5.5.5 Requirements for Timestamping of Records

Controls as defined in the TrustFactory CP

5.5.6 Archive Collection System (Internal or External)

Controls as defined in the TrustFactory CP

5.5.7 Procedures to Obtain and Verify Archive Information

Controls as defined in the TrustFactory CP.

5.6 Key Changeover

Towards the end of the SSL Issuing CA private key's lifetime, in accordance with Section 6.3.2, a new CA signing key pair is commissioned by the TrustFactory PA and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both keys may be concurrently active. Private Keys used to sign previous Subscriber Certificates are maintained until such time as all Subscriber Certificates have expired.

Certificate Subject information may also be modified and Certificate profiles may be altered to adhere to best practices.

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Controls are as defined in the TrustFactory CP

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

Controls are as defined in the TrustFactory CP

5.7.3 Recovery Procedures After Key Compromise

Controls are as defined in the TrustFactory CP



5.7.4 Business Continuity Capabilities after a Disaster

Controls are as defined in the TrustFactory CP

5.8 CA or RA Termination

Controls are as defined in the TrustFactory CP



6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The signing key pair for the TrustFactory SSL Issuing CA was created during the initial startup of the CA application and is protected by the master keys for the TrustFactory SSL Issuing CA. Hardware key generation is used which is compliant to FIPS 140-2 level 3 and uses FIPS 186-2 key generation techniques.

TrustFactory SSL Issuing CA generates its CA Key Pairs under the following conditions:

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

6.1.1.2 RA Key Pair Generation

Not applicable

6.1.1.3 Subscriber Key Pair Generation

TrustFactory SSL Issuing CA does not provide subscriber key generation or key management services.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

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

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

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

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

6.1.5 Key Sizes

The TrustFactory SSL Issuing CA Certificate utilizes a key size of 4096 bits (RSA) with hash algorithm SHA-256.

Subscriber Certificates meet the following requirements for algorithm type and key size.

(1) Subscriber Certificates

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

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



6.1.6 Public Key Parameters Generation and Quality Checking

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

6.1.7 Key Usage Purposes

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

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

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

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

Any other use not specified above is prohibited.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Controls as per the TrustFactory CP

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

Controls as per the TrustFactory CP

6.2.3 Private Key Escrow

Controls as per the TrustFactory CP

6.2.4 Private Key Backup

Controls as per the TrustFactory CP

6.2.5 Private Key Archival

Controls as per the TrustFactory CP

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Controls as per the TrustFactory CP

6.2.7 Private Key Storage on Cryptographic Module

Controls as per the TrustFactory CP

6.2.8 Method of Activating Private Key

Controls as per the TrustFactory CP

6.2.9 Method of Deactivating Private Key

Controls as per the TrustFactory CP

6.2.10 Method of Destroying Private Key

Controls as per the TrustFactory CP

6.2.11 Cryptographic Module Capabilities

See Section 6.2.1



6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

TrustFactory SSL Issuing CA archives Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

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

TrustFactory SSL Issuing CA complies with the Baseline Requirements with respect to the maximum Validity Period.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of TrustFactory SSL Issuing CA activation data used to activate TrustFactory SSL Issuing CA Private Keys are made during a key ceremony (Refer to Section 6.1.1). Activation data is generated automatically by the appropriate HSM. It is then delivered to a holder of a share of the key who is a person in a trusted role. The delivery method maintains the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

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

6.4.3 Other Aspects of Activation Data

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

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Controls as per the TrustFactory CP.

6.5.2 Computer Security Rating

Controls as per the TrustFactory CP.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

Controls as per the TrustFactory CP

6.6.2 Security Management Controls

Controls as per the TrustFactory CP.

6.6.3 Lifecycle Security Controls

Controls as per the TrustFactory CP.

6.7 Network Security Controls

Controls as per TrustFactory CP

6.8 Time Stamping

Controls as per TrustFactory CP





7.0 Certificate, CRL, and OCSP Profiles

Typical content of information published on a TrustFactory SSL Certificate may include but is not limited to the following elements of information:

- Serial number
- Signature algorithm
- Signature hash algorithm
- Issuer
- Valid from
- Valid to
- Subject
- Public key
- Basic Constraints
- Key Usage
- Authority Information Access
- Certificate Policies
- CRL Distribution Points
- Extended key usage

7.1 Certificate Profile

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

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

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

7.1.2.1. Root CA Certificate

Not applicable

7.1.2.2. Subordinate CA Certificate

The following applies to the TrustFactory SSL Issuing CA – the specific content of the fields in the certificate can be found in the profile in Annexure A:

- a. `certificatePolicies`
This extension is present and not set as critical.
- b. `cRLDistributionPoints`
This extension is present and is not set as critical, and it contains the HTTP URL of the CA's CRL service.
- c. `authorityInformationAccess`
This extension is present and is not set as critical, and it contains the HTTP URL of the Issuing CA's OCSP responder (`accessMethod = 1.3.6.1.5.5.7.48.1`).
- d. `basicConstraints`
This extension is present and is set as a critical extension. `CA` field is set true.
- e. `keyUsage`
This extension is present and is set as a critical extension.
Bit positions for `digitalSignature`, `keyCertSign` and `cRLSign` are set.
- f. `extkeyUsage` (optional)
This extension is not present

7.1.2.3. Subscriber Certificates

The following applies to the Subscriber certificates – the specific content of the fields in the certificate can be found in the profiles in Annexure A::

- a. `certificatePolicies`
 - This extension is not set as critical.



- certificatePolicies:policyIdentifier is populated in accordance to Section 1.2
- b. cRLDistributionPoints
 - This extension is not set as critical, and it contains the HTTP URL of the CA's CRL service.
- c. authorityInformationAccess
 - This extension is not set as critical, and it contains the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2)
- d. keyUsage
 - Populated based on certificate type described in Section 1.4.1 and set in accordance with RFC 5280
- e. extKeyUsage (required)
 - Populated based on certificate type described in Section 1.4.1 and set in accordance with RFC 5280

7.1.2.4. All Certificates

All other fields and extensions are be set in accordance with RFC 5280. The TrustFactory SSL Issuing CA will not issue a Certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in section 7.1.2.1, 7.1.2.2, or 7.1.2.3.

TrustFactory SSL Issuing CA will not issue a Certificate with:

- a. Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network), unless:
 - i. such value falls within an OID arc for which the Applicant demonstrates ownership, or
 - ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or
- b. semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA (such as including extendedKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.2.5. Application of RFC 5280

For purposes of clarification, a Precertificate, as described in RFC 6962 – Certificate Transparency, shall not be considered to be a “certificate” subject to the requirements of RFC 5280 under this CPS.

7.1.3 Algorithm Object Identifiers

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

7.1.4 Name Forms

7.1.4.1. Issuer Information

TrustFactory SSL Issuing CA issues Certificates with name forms compliant to RFC 5280. Name chaining of a Certificate is performed by matching the content of the Certificate Issuer Distinguished Name field of the Certificate to the Subject Distinguished Name of the Issuing CA that issued the Certificate.

7.1.4.2. Subject Information – Subscriber Certificates

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

TrustFactory SSL Issuing CA does not allow the following in certificates:

- a) IP Addresses or Internal Names (Local name) in the subjectAlternativeName extension or subject commonName field.
- b) underscore characters (“_”) are not permitted in dNSName entries

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

Certificate Field	Criteria
extensions:subjectAltName	Required field. Contains each Fully-Qualified Domain Name that has been validated as per Section 3.2.2.4 or 3.2.2.5
subject:commonName (OID 2.5.4.3)	Optional Contains one of the values contained in the Certificate's subjectAltName extension
subject:organizationName (OID 2.5.4.10)	Optional Contains Subscriber Organisation name or DBA name as verified under Section 3.2.2.2
subject:localityName (OID: 2.5.4.7)	Required if the subject:organizationName field is present and the subject:stateOrProvinceName field is absent. Optional if the subject:stateOrProvinceName field and the subject:organizationName are present. Prohibited if the subject:organizationName is absent. Contains the Subject's locality information as verified under Section 3.2.2.1.
subject:stateOrProvinceName (OID: 2.5.4.8)	Required if the subject:organizationName field is present and subject:localityName field is absent. Optional if the subject:localityName field and the subject:organizationName field are present. Prohibited if the subject:organizationName field, is absent. Contains the Subject's state or province information as verified under Section 3.2.2.1.
subject:countryName (OID: 2.5.4.6)	Required if the subject:organizationName field is present. Optional if the subject:organizationName field is absent Contains the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.2.1.
subject:organizationalUnitName	Optional Information in this field is not validated.

All other subject fields (givenName, surname, streetAddress or postalCode) are not permitted.

Add in IDN handling when ready??

7.1.4.3. Subject Information – Root Certificates and Subordinate CA Certificates

Not applicable. TrustFactory SSL Issuing CA does not issue Root or Subordinate CA certificates.

7.1.5 Name Constraints

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

7.1.6 Certificate Policy Object Identifier

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

7.1.6.1. Reserved Certificate Policy Identifiers

TrustFactory SSL Issuing CA includes where applicable, the following CAB Forum Reserved Certificate Policy identifiers as a means of asserting compliance with the Requirements as follows:

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1), if the Certificate complies with these Requirements but lacks Subject Identity Information that is verified in accordance with Section 3.2.2.1 or Section 3.2.3.

If the Certificate asserts the policy identifier of 2.23.140.1.2.1, then it MUST NOT include organizationName, givenName, surname, streetAddress, localityName, stateOrProvinceName, or postalCode in the Subject field.

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2), if the Certificate complies with these



Requirements and includes Subject Identity Information that is verified in accordance with Section 3.2.2.1.

If the Certificate asserts the policy identifier of 2.23.140.1.2.2, then it MUST also include organizationName, localityName (to the extent such field is required under Section 7.1.4.2.2), stateOrProvinceName (to the extent such field is required under Section 7.1.4.2.2), and countryName in the Subject field.

7.1.6.2. Root CA Certificates

Not applicable.

7.1.6.3. Subordinate CA Certificates

TrustFactory SSL Issuing CA is an Affiliate of its issuer TrustFactory SSL Root CA, and asserts the “anyPolicy” identifier 2.5.29.32.0 to indicate certificate is issued and managed in compliance with the Requirements.

7.1.6.4. Subscriber Certificates

TrustFactory SSL Issuing CA includes the following CAB Forum reserved certificate policy identifiers in its Subscriber Certificates’ certificatePolicies extension to assert compliance with the Requirements:

- i. OID 2.23.140.1.2.1 included in DomainPass certificates to assert domain validated in accordance with the Requirements.

DomainPass certificates do not include organizationName, givenName, surname, streetAddress, localityName, stateOrProvinceName, or postalCode in the Subject field

- ii. OID 2.23.140.1.2.2 included in OrganizationPass certificates to assert domain and organization validated in accordance with the Requirements.

OrganizationPass certificates must also include organizationName, localityName (to the extent such field is required under Section 7.1.4.2), stateOrProvinceName (to the extent such field is required under Section 7.1.4.2), and countryName in the Subject field.

7.1.7 Usage of Policy Constraints Extension

No requirements specified.

7.1.8 Policy Qualifiers Syntax and Semantics

No requirements specified.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No requirements specified.

7.2 CRL Profile

7.2.1 Version Number(s)

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

- **Issuer:**
 - CN = TrustFactory SSL Issuing Certificate Authority
 - OU = TrustFactory PKI Operations
 - O = TrustFactory(Pty)Ltd
 - L = Johannesburg
 - S = Gauteng
 - C = ZA
- **Effective date** Date and Time issued
- **Next update** Date and Time of next issue
- **Signature Algorithm** sha256RSA



- **Signature Hash Algorithm** sha256
- **Serial Number(s)** List of revoked serial numbers
- **Revocation Date** Date of Revocation

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:

- **CRL Number** Monotonically increasing serial number for each CRL
- **Authority Key Identifier** AKI of the Issuing CA for chaining/validation requirements

7.3 OCSP Profile

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

7.3.1 Version Number(s)

TrustFactory SSL Issuing CA issues Version 1 OCSP responses

7.3.2 OCSP Extensions

TrustFactory SSL Issuing CA issues OCSP responses with following fields:

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

An OCSP request must contain the following data:

- Protocol version
- Service request
- Target Certificate identifier

8.0 Compliance Audit and Other Assessments

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

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

8.1 Frequency and Circumstances of Assessment

Controls as per TrustFactory CP.

8.2 Identity/Qualifications of Assessor

Controls as per TrustFactory CP

8.3 Assessor's Relationship to Assessed Entity



Controls as per TrustFactory CP

8.4 Topics Covered by Assessment

Controls as per TrustFactory CP.

8.5 Actions Taken as a Result of Deficiency

Controls as per TrustFactory CP.

8.6 Communications of Results

Controls as per TrustFactory CP.

8.7 Self Audits

Controls as per TrustFactory CP.

9.0 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Controls as per the TrustFactory CP

9.1.2 Certificate Access Fees

Controls as per the TrustFactory CP

9.1.3 Revocation or Status Information Access Fees

Controls as per the TrustFactory CP

9.1.4 Fees for Other Services

Controls as per the TrustFactory CP

9.1.5 Refund Policy

Controls as per the TrustFactory CP

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Controls as per the TrustFactory CP

9.2.2 Other Assets

Controls as per the TrustFactory CP

9.2.3 Insurance or Warranty Coverage for End Entities

Controls as per the TrustFactory CP

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Controls as per the TrustFactory CP

9.3.2 Information Not Within the Scope of Confidential Information

Controls as per the TrustFactory CP

9.3.3 Responsibility to Protect Confidential Information

Controls as per the TrustFactory CP.



9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Controls as per the TrustFactory CP.

9.4.2 Information Treated as Private

Controls as per the TrustFactory CP.

9.4.3 Information Not Deemed Private

Controls as per the TrustFactory CP.

9.4.4 Responsibility to Protect Private Information

Controls as per the TrustFactory CP.

9.4.5 Notice and Consent to Use Private Information

Controls as per the TrustFactory CP.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Controls as per the TrustFactory CP.

9.4.7 Other Information Disclosure Circumstances

Controls as per the TrustFactory CP.

9.5 Intellectual Property rights

Controls as per the TrustFactory CP

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Controls as per the TrustFactory CP

9.6.2 RA Representations and Warranties

Controls as per the TrustFactory CP

9.6.3 Subscriber Representations and Warranties

Controls as per the TrustFactory CP

•

9.6.4 Relying Party Representations and Warranties

Controls as per the TrustFactory CP.

9.6.5 Representations and Warranties of Other Participants

Controls as per the TrustFactory CP.

9.7 Disclaimers of Warranties

Controls as per the TrustFactory CP

9.8 Limitations of Liability

Controls as per the TrustFactory CP

9.9 Indemnities

Controls as per the TrustFactory CP



9.10 Term and Termination

9.10.1 Term

Controls as per the TrustFactory CP.

9.10.2 Termination

Controls as per the TrustFactory CP.

9.10.3 Effect of Termination and Survival

Controls as per the TrustFactory CP.

9.11 Individual Notices and Communications with Participants

Controls as per the TrustFactory CP

9.12 Amendments

9.12.1 Procedure for Amendment

Controls as per the TrustFactory CP.

9.12.2 Notification Mechanism and Period

Controls as per the TrustFactory CP.

9.12.3 Circumstances Under Which OID Must be Changed

Controls as per the TrustFactory CP.

9.13 Dispute Resolution Provisions

Controls as per the TrustFactory CP.

9.14 Governing Law

Controls as per the TrustFactory CP.

9.15 Compliance with Applicable Law

Controls as per the TrustFactory CP.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Controls as per the TrustFactory CP.

9.16.2 Assignment

Controls as per the TrustFactory CP.

9.16.3 Severability

Controls as per the TrustFactory CP.

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

Controls as per the TrustFactory CP

9.17 Other Provisions

Controls as per the TrustFactory CP



Annexure A: SSL CA Certificate Profiles

TrustFactory SSL Issuing CA – Certificate Profile

V1 Fields	
Version	V3
Serial number	
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CN=TrustFactory SSL Root Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA
Validity	15 years
Subject	CN = TrustFactory SSL Issuing Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA
Public key	RSA (4096 bits)
Critical Extensions	
Basic Constraints	Subject Type=CA
	Path Length Constraint=0
Key Usage	Certificate Signing Off-line CRL Signing CRL Signing Digital Signature
Extensions	
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.trustfactory.net/tf-ssl-issuing
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.5.29.32.0 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.trustfactory.net/repository
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://www.trustfactory.net/crl/tf-ssl-issuing.crl
Properties	
Thumbprint algorithm	SHA1



DOMAINPASS Certificate Profile

V1 Fields	
Version	V3
Serial number	
Signature algorithm	sha256RSA
Signature algorithm hash	sha256
Issuer	CN = TrustFactory SSL Issuing Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA
Validity	1 or 2 years
Subject	CN = domain name
Public key	RSA (minimum 2048 bits)
Extensions	
Basic Constraints	Subject Type=EndEntity
	Path Length Constraint=None
Key Usage	Digital Signature Key Encipherment
Extended key usage (property)	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.trustfactory.net/tf-ssl-issuing [2] Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= https://www.trustfactory.net/repository/tf-online-ssl.crt
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.50318.2.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.trustfactory.net/repository [2]Policy Identifier= 2.23.140.1.2.1
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.trustfactory.net/crl/tf-ssl-subscriber.crl
Subject Alternative Name	required – first domain name validated (upto 100 for Premium Certs)
Properties	
Thumbprint algorithm	SHA1



ORGANISATIONPASS Certificate Profile

V1 Fields	
Version	V3
Serial number	
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CN = TrustFactory SSL Issuing Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA
Validity	1 or 2 years
Subject	CN = <i>domain name</i> OU = <i>(optional)</i> O = <i>organisation name</i> L = <i>registered address city</i> ST = <i>(optional if L is present)</i> C = <i>registered address country</i>
Public key	RSA (<i>minimum 2048 bits</i>)
Extensions	
Basic Constraints	Subject Type=EndEntity
	Path Length Constraint=None
Key Usage	Digital Signature Key Encipherment
Extended key usage (property)	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.trustfactory.net/tf-ssl-issuing [2] Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= https://www.trustfactory.net/repository/tf-online-ssl.crt
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.50318.2.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.trustfactory.net/repository [2]Policy Identifier= 2.23.140.1.2.2
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.trustfactory.net/crl/tf-ssl-subscriber.crl
Subject Alternative Name	<i>required – first domain name validated (upto 100 for Premium Certs)</i>
Properties	
Thumbprint algorithm	SHA1