OISTE Foundation

OISTE Global Trust Model

Root CA Certification Practices Statement (CPS)

Date: 20/2/2021	**Version**: 3.2
Status: FINAL	**No. Of Pages**: 60
OID: 2.16.756.5.14.7.1	**Classification**: PUBLIC
File: OGTM - OISTE Foundation CPS.v3.2-REDLINE.docx	
Published by: OISTE Policy Approval Authority	

.

Documentation management

Document Approval

Version	PAA Representative #1	PAA Representative #2
3.2	Name: Signature:	Name: Signature:

Version history

Version	Date	Comments
1.0	1/12/2005	First version
2.0	1/5/2015	Major change to adopt RFC3647 and CABF compliance
3.0	25/2/2019	Major change to adopt new CP / CPS documentation framework
3.1	23/2/2020	Minor changes to adapt compliance wording
3.2	20/2/2021	Annual review

Contents

1 Introductions 9

1.1 Overview 9
1.1.1 The OGTM CP/CPS Documentation Framework 10

1.2 Document Name and Identification 10

1.3 PKI Participants 11
1.3.1 Certification authorities 11
1.3.2 Registration authorities 12
1.3.3 Subscribers 13
1.3.4 Relying parties 13
1.3.5 Other participants 13

1.4 Certificate Usage 13
1.4.1 Appropriate Certificate Uses 13
1.4.2 Prohibited certificate uses 14

1.5 Policy Administration 14
1.5.1 Organization administering the document 14
1.5.2 Contact Person (Contact Information) 14
1.5.3 Person determining CPS suitability for the policy 14
1.5.4 CPS approval procedures 14

1.6 Definitions and Acronyms 14

2 Publication and Repository Responsibilities 15

2.1 Repositories 15

2.2 Publication 15
2.2.1 Statement on Compliance with CA/Browser Forum requirements 15

2.3 Time or frequency of publication 15

2.4 Access control on repositories 15

3 Identification and Authentication 16

3.1 Naming 16
3.1.1 Types of names 16
3.1.2 Need for names to be meaningful 16
3.1.3 Anonymity of subscribers and pseudonyms 16
3.1.4 Rules for interpreting various name forms 16
3.1.5 Uniqueness of names 16
3.1.6 Recognition, authentication, and role of trademarks 16

3.2 Initial Identity Validation 17
3.2.1 Method to prove possession of private key 17
3.2.2 Authentication of organization identity 17
3.2.3 Authentication of individual identity 17
3.2.4 Non-verified subscriber information 17
3.2.5 Validation of authority 17
3.2.6 Criteria for interoperation 17

3.3 Identification and Authentication for Re-key Requests 18
3.3.1 Identification and authentication for routine re-key 18
3.3.2 Identification and authentication for re-key after revocation 18

3.4 Identification and Authentication for Revocation Requests 18

4 Certificate Life-Cycle Operational Requirements 19

4.1 Certificate Application 19
4.1.1 Who can submit a certificate application 19
4.1.2 Enrolment process and responsibilities 19

4.2 Certificate Application Processing 19
4.2.1 Performing identification and authentication functions 19
4.2.2 Approval or rejection of certificate applications 20
4.2.3 Time to process certificate applications 20

4.3 Certificate Issuance 20
4.3.1 CA actions during certificate issuance 20
4.3.2 Notifications to subscriber by the CA of issuance of certificate 20

4.4 Certificate Acceptance 20
4.4.1 Conduct constituting certificate acceptance 20
4.4.2 Publication of the certificate by the CA 20
4.4.3 Notification of certificate issuance by the CA to other entities 20

4.5 Key Pair and Certificate Usage 21
4.5.1 Subscriber private key and certificate usage 21
4.5.2 Relying party public key and certificate usage 21

4.6 Certificate Renewal 21
4.6.1 Circumstance for certificate renewal 21
4.6.2 Who may request renewal 21
4.6.3 Processing certificate renewal requests 21
4.6.4 Notification of new certificate issuance to subscriber 21
4.6.5 Conduct constituting acceptance of a renewal certificate 21
4.6.6 Publication of the renewal certificate by the CA 21
4.6.7 Notification of certificate issuance by the CA to other entities 22

4.7 Certificate Re-key 22
4.7.1 Circumstance for certificate re-key 22
4.7.2 Who may request certification of a new public key 22
4.7.3 Processing certificate re-keying requests 22
4.7.4 Notification of new certificate issuance to subscriber 22
4.7.5 Conduct constituting acceptance of a re-keyed certificate 22
4.7.6 Publication of the re-keyed certificate by the CA 22
4.7.7 Notification of certificate issuance by the CA to other entities 22

4.8 Certificate Modification 22
4.8.1 Circumstance for certificate modification 22
4.8.2 Who may request certificate modification 23
4.8.3 Processing certificate modification requests 23
4.8.4 Notification of new certificate issuance to subscriber 23
4.8.5 Conduct constituting acceptance of modified certificate 23
4.8.6 Publication of the modified certificate by the CA 23
4.8.7 Notification of certificate issuance by the CA to other entities 23

4.9 Certificate Revocation and Suspension 23
4.9.1 Circumstances for revocation 23
4.9.2 Who can request revocation 25
4.9.3 Procedure for revocation request 25
4.9.4 Revocation request grace period 25
4.9.5 Time within which CA must process the revocation request 25
4.9.6 Revocation checking requirement for relying parties 26
4.9.7 CRL issuance frequency 26
4.9.8 Maximum latency for CRLs 26

4.9.9 On-line revocation/status checking availability 26
4.9.10 On-line revocation checking requirements 26
4.9.11 Other forms of revocation advertisements available 26
4.9.12 Special requirements regarding key compromise 26
4.9.13 Circumstances for suspension 27
4.9.14 Who can request suspension 27
4.9.15 Procedure for suspension request 27
4.9.16 Limits on suspension period 27

4.10 Certificate Status Services 27
4.10.1 Operational characteristics 27
4.10.2 Service availability 27
4.10.3 Optional features 27

4.11 End of Subscription 27

4.12 Key Escrow and Recovery 28
4.12.1 Key escrow and recovery policy and practices 28
4.12.2 Session key encapsulation and recovery policy and practices 28

5 Management, Operational, and Physical Controls 29

5.1 Physical Security Controls 29
5.1.1 Site location and construction 29
5.1.2 Physical access 29
5.1.3 Power and air conditioning 30
5.1.4 Water exposures 30
5.1.5 Fire prevention and protection 30
5.1.6 Media storage 30
5.1.7 Waste disposal 30
5.1.8 Backup 30

5.2 Procedural Controls 30
5.2.1 Trusted roles 30
5.2.2 Number of persons required per task 31
5.2.3 Identification and authentication for each role 31
5.2.4 Roles requiring separation of duties 31

5.3 Personnel Security Controls 31
5.3.1 Qualifications, experience, and clearance requirements 32
5.3.2 Background check procedures 32
5.3.3 Training requirements 32
5.3.4 Retraining frequency and requirements 32
5.3.5 Job rotation frequency and sequence 32
5.3.6 Sanctions for unauthorized actions 32
5.3.7 Independent contractor requirements 32
5.3.8 Documentation supplied to personnel 33
5.3.9 Contract termination and assigned role change procedures 33

5.4 Audit Logging Procedures 33
5.4.1 Types of events recorded 33
5.4.2 Frequency of processing log 34
5.4.3 Retention period for audit log 34
5.4.4 Protection of audit log 34
5.4.5 Audit log backup procedures 34
5.4.6 Audit collection system (internal vs. external) 34
5.4.7 Notification to event-causing subject 34
5.4.8 Vulnerability assessments 34

5.5 Records Archival 34

5.5.1 Types of records archived 34
5.5.2 Retention period for archive 35
5.5.3 Protection of archive 35
5.5.4 Archive backup procedures 35
5.5.5 Requirements for time-stamping of records 35
5.5.6 Archive collection system (internal or external) 35
5.5.7 Procedures to obtain and verify archive information 35

5.6 Key Changeover 35

5.7 Compromise and Disaster Recovery 36
5.7.1 Incident and compromise handling procedures 36
5.7.2 Computing resources, software, and/or data are corrupted 36
5.7.3 Entity private key compromise procedures 36
5.7.4 Business continuity capabilities after a disaster 36

5.8 CA or RA Termination 36

6 Technical Security Controls 38

6.1 Key Pair Generation and Installation 38
6.1.1 Key pair generation 38
6.1.2 Private key delivery to subscriber 38
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 39
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 39

6.2 Private Key Protection and Cryptographic Module Engineering Controls 39
6.2.1 Cryptographic module standards and controls 39
6.2.2 Private key (n out of m) multi-person control 39
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 41
6.2.11 Cryptographic Module Rating 41

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 42
6.4.2 Activation data protection 42
6.4.3 Other aspects of activation data 42

6.5 Computer Security Controls 42
6.5.1 Specific computer security technical requirements 42
6.5.2 Computer security rating 42

6.6 Life Cycle Security Controls 42
6.6.1 System development controls 43
6.6.2 Security management controls 43
6.6.3 Life cycle security controls 43

6.7 Network Security Controls 43

6.8 Time-stamping 43

7 Certificate and CRL Profiles 44

7.1 Certificate Profile 44
7.1.1 Version number(s) 44
7.1.2 Certificate extensions 44
7.1.3 Algorithm object identifiers 44
7.1.4 Name forms 44
7.1.5 Name constraints 44
7.1.6 Certificate policy object identifier 45
7.1.7 Usage of Policy Constraints extension 45
7.1.8 Policy qualifiers syntax and semantics 45
7.1.9 Processing semantics for the critical Certificate Policies extension 45

7.2 CRL Profile 45
7.2.1 Version number(s) 45
7.2.2 CRL Profile and CRL entry extensions 45

7.3 OCSP Profile 45
7.3.1 Version number(s) 46
7.3.2 OCSP extensions 46

8 Compliance Audit and Other Assessment 47

8.1 Frequency or 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 47

8.5 Actions taken as a result of deficiency 47

8.6 Communication of results 48

9 Other Business and Legal Matters 49

9.1 Fees 49
9.1.1 Certificate issuance or renewal fees 49
9.1.2 Certificate access fees 49
9.1.3 Revocation or status information access fees 49
9.1.4 Fees for other services 49
9.1.5 Refund policy 49

9.2 Financial Responsibility 49
9.2.1 Insurance coverage 50
9.2.2 Other assets 50
9.2.3 Insurance or warranty coverage for end-entities 50

9.3 Confidentiality of Business Information 50
9.3.1 Scope of confidential information 50
9.3.2 Information not within the scope of confidential information 50
9.3.3 Responsibility to protect confidential information 51

9.4 Privacy of Personal Information 51
9.4.1 Privacy plan 51
9.4.2 Information treated as private 51
9.4.3 Information not deemed private 51
9.4.4 Responsibility to protect private information 51
9.4.5 Notice and consent to use private information 51

9.4.6 Disclosure pursuant to judicial or administrative process 52
9.4.7 Other information disclosure circumstances 52
9.5 Intellectual Property Rights 52
9.6 Representations and Warranties 52
9.6.1 CA representations and warranties 52
9.6.2 RA representations and warranties 53
9.6.3 Subscriber representations and warranties 53
9.6.4 Relying party representations and warranties 54
9.6.5 Representations and warranties of other participants 54
9.7 Disclaimers of Warranties 54
9.8 Limitations of Liability 54
9.9 Indemnities 54
9.10 Term and Termination 55
9.10.1 Term 55
9.10.2 Termination 55
9.10.3 Effect of termination and survival 55
9.11 Individual notices and communications with participants 55
9.12 Amendments 55
9.12.1 Procedure for amendment 55
9.12.2 Notification mechanism and period 56
9.12.3 Circumstances under which OID must be changed 56
9.13 Dispute Resolution Procedures 56
9.14 Governing Law 56
9.15 Compliance with Applicable Law 56
9.16 Miscellaneous Provisions 56
9.16.1 Entire agreement 56
9.16.2 Assignment 56
9.16.3 Severability 56
9.16.4 Enforcement (attorneys' fees and waiver of rights) 57
9.16.5 Force Majeure 57
9.17 Other Provisions 57
10 Annex A: Glossary 58
11 Annex B: OID Inventory 59

1 Introductions

1.1 Overview

This Certification Practice Statement (CPS) describes the practices followed with regard to the management of the lifecycle the Certification Authorities adhered to the OISTE Global Trust Model.

The main two legal entities involved in the control and operation of the Trust Model are:

- **OISTE Foundation**. The International Organization for Secure Electronic Transactions ("IOSET" or "OISTE"), a Swiss non-profit foundation established in 1998, and recognized with an "Special Consultative Status" by the United Nations. The OISTE Foundation maintains a Policy Approval Authority (OFPAA or PAA) that drafts, approves and revises the policies to which WISeKey is bound to comply with under its operator contract. The PAA is composed of members of the community to which OISTE provides its Certification Authority Services, resulting in a virtuous cycle for trust management.
- **WISeKey**. WISeKey is referenced in this document as the short name for the entities "WISeKey International Holding Ltd.", "WISeKey SA" or other members of the WISeKey Holding that are mandated by OISTE to host and operate the Root Certification Authorities and the technical infrastructures required to maintain the PKI at the appropriate operational level. WISeKey also operates as a "Subordinate Certification Authority" under the OISTE Roots, according to practices disclosed in the appropriate CPS document published by WISeKey and endorsed by OISTE.

The OISTE Global Trust Model (**OGTM from now on**) has been designed and are operated in accordance with the broad strategic direction of international PKI (Public Key Infrastructure) standards as well as their application to concrete identity frameworks in different domains (e.g. ID cards, passports, health cards, Internet of Things) and is intended to serve as a common Trust Model for Certification Authorities worldwide that comply with OISTE requirements.

The technologies, infrastructures, practices, and procedures implemented by the **OGTM** have been designed with explicit standards of security in mind based on the requirements approved by OISTE.

The OISTE Foundation, under Swiss law, cannot belong to any individual or company. It is subject to annual supervision by the Swiss Federal Government and audited annually by independent auditors. Such supervision and audit require the foundation to pursue the objectives that have been set out for it, which includes the promotion of security in electronic communications worldwide.

This document is developed per the recommendations found in the document **RFC3647***, developed by the Internet Engineering Task Force (IETF)*, which has been adopted as a worldwide-recognized standard framework to document the Certifications Practice Statement and related Certificate Policies disclosed by a Certification Services Provider.

The purpose of this document is to disclose the Practices and Policies adopted in the **OGTM** for the issuance of digital certificates. It is organized in the following sections:

1. Introductions – This section. Introduces the **OGTM** and this document.
2. Publication and Repositories Responsibilities – Describes the publication policies for the certificates affected by this document, and the publication of this document itself.
3. Identification and Authentication – Discloses the rules for subscriber naming and required authentication policies.
4. Certificate Life-Cycle Operational Requirements – This section describes the different phases in the Life-Cycle of certificates and their requirements.

5. Management, Operational and Physical Controls – Describes the controls enforced in the **OGTM** to provide adequate trust levels in the certificates issued under the Trust Model.
6. Technical Security Controls – Discloses the security controls adopted in the **OGTM**.
7. Certificate and CRL Profiles – Describes the technical details of the different certificate types issued under the **OGTM**.
8. Compliance Audit and other Assessment – Discloses the audit policies followed in the **OGTM** to ensure that the participant fulfils the security and quality requirements.
9. Other Business and Legal Matters – This section exposes the commercial, legal and contractual aspects involved in the usage of certificates issued in the **OGTM**.

1.1.1 The OGTM CP/CPS Documentation Framework

The main information disclosed by the **OGTM** in order to expose its practices and policies in the issuance and usages of digital certificates are:

- The Certification Practices Statement (CPS) –The CPS is a statement of the practices that every Certification Authority operating under the **OGTM** Trust Model employs in issuing, managing, revoking, and renewing or re-keying certificates. This CPS document discloses the stipulations related to the issuance of Subordinate CA Certificates, assigned to entities acting as "Issuing Certification Authorities" under the **OGTM**. Those entities must publish their own CPS to disclose the stipulations related to end-entity certification practices.
- A number of Certificate Policies (CP) – each being a named set of rules that indicates the applicability of a type or profile of certificate to a particular community and/or class of application with common security requirements. ***Any explicit mention to a CP document must be understood as referring to the appropriate CP document for the certificate type being evaluated***.

The CP/CPS hierarchy and documentation framework is regulated by the OISTE Foundation and disclosed in http://www.oiste.org/repository.

The CPS and CP documents follow the same structure, the second being a specialization of the CPS for a certain type of certificate. Common policies and practices are only published within the CPS. For the convenience of readers of this CPS, the sections that are generally specified within a particular CP are clearly noted with the sentence: *"As stipulated in the appropriate CP"*.

For the shake of simplicity, OISTE is not publishing a specific CP for the "Subordinate CA" Certificate Profiles but integrating the appropriate details and stipulation in this "Root CPS".

1.2 Document Name and Identification

Name	OGTM Root CA Certification Practices Statement
Version	3.2
OID	2.16.756.5.14.7.1
Issuance date	20/2/2021
Location	This document can be found at http://www.oiste.org/repository

1.3 PKI Participants

1.3.1 Certification authorities

The current full list of Certification Authorities that have been authorized by OISTE to operate under the **OGTM** is disclosed in **http://www.oiste.org/repository**.

1.3.1.1 Root Certification Authorities

- "**WISeKey OISTE Global Root CA**". This is the first level Certification Authority; its role is to establish the Root of the Trust Model, or **OGTM**. This Certification Authority does not issue certificates for end entities, but only for the Issuing and Intermediary Certification Authorities (as described below). The certificates of these Root Certification Authorities are self-signed and currently the **OGTM** maintains two Root Certification Authorities, in order to provide support for two parallel hierarchies. The identification data of these Root CA are included in the following tables:

Short name	OWGTM Root CA GA
Distinguished Name	CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright © 2005, O=WISeKey, C=CH
SHA-1 Fingerprint	59 22 A1 EA 5A EA 16 35 21 F8 98 3ª 6A 46 46 B0 44 1B 0F A9
Issued by	<SELF-SIGNED>
Issuance date	11 of December, 2005
Expiration date	11 of December, 2037
Location	This certificate, in the common standard formats, can be found in http://www.oiste.org/repository

Short name	OWGTM Root CA GB
Distinguished Name	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH
SHA-1 Fingerprint	0F F9 40 76 18 D3 D7 6A 4B 98 F0 A8 35 9E 0C FD 27 AC CC ED
Issued by	<SELF-SIGNED>
Issuance date	1 of December, 2014
Expiration date	1 of December, 2039
Location	This certificate, in the common standard formats, can be found in http://www.oiste.org/repository

Short name	OWGTM Root CA GC
Distinguished Name	CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH
SHA-1 Fingerprint	E0 11 84 5E 34 DE BE 88 81 B9 9C F6 16 26 D1 96 1F C3 B9 31

Issued by	<SELF-SIGNED>
Issuance date	9 of May, 2017
Expiration date	9 of May, 2042
Location	This certificate, in the common standard formats, can be found in http://www.oiste.org/repository

Important clarification about the "Organization" field in Root CA Certificates

For historical reasons, Root CA certificates created before 2019 have been named using the "WISeKey" brand in the Organization field of the "Subject Name" extension, but it must be always understood that the entity which is owning the Root CAs is the OISTE Foundation, while WISeKey acts as an operator of the Trust Model.

1.3.1.2 Intermediary Certification Authorities

Intermediate Certification Authorities, also named "Policy Certification Authorities" are used, when adequate, to segregate different branch of the Trust Model, by certificate types or CA owner, being totally acceptable having Issuing CA directly signed by the OISTE Roots.

The OISTE Foundation currently doesn't own any Intermediary CA and those existing are owned, operated, and disclosed by the authorized subordinated entities endorsed by OISTE to act as subordinated Certification Authorities.

1.3.1.3 Issuing Certification Authorities

OGTM Issuing Certification Authorities. End Entity certificates are issued by a particular "Issuing CA" that was generated under "OGTM Root CA" or a particular "Policy CA", depending on the characteristics of that Entity. These Issuing CAs are owned, operated, and disclosed by the authorized subordinated entities endorsed by OISTE to act as subordinated Certification Authorities. Each of those Issuing CAs are accredited to issue a certain type (or types) of certificates, each conforming to a "Certificate Policy" (CP) approved by the **OGTM**. A list of accredited Subordinate CAs, and allowed CP, is disclosed in the web repository available at http://www.oiste.org/repository.

Issuing Certification Authorities operated by an **OWGTM** affiliate[1] must follow an accreditation process before starting their operations. In particular, WISeKey, as designated operator by the **OWGTM**, will manage all the commercial and technical aspects of the affiliation. The affiliate will be subject of a periodic audit to ensure the compliance with this CPS and all applicable regulations.

1.3.2 Registration authorities

The OISTE Foundation doesn't issue end-entity certificates, and therefore the Registration Authorities aren't in scope of this CPS.

The stipulations related to Registration Authorities, therefore, are considered in the CPS published by the Authorized Subordinate Certification Authorities, operating under the OISTE Roots CAs.

[1] WISeKey is also considered an affiliate, being also the main operator of the **OGTM**.

1.3.3 Subscribers

The OISTE Foundation doesn't operate any Issuing Certification Authority, and therefore the stipulations related to the certificate subscribers are considered in the CPS published by the Authorized Subordinate Certification Authorities, operating under the OISTE Roots CAs.

1.3.4 Relying parties

All persons and entities that trust the certificates issued by certification authorities operating under the **OGTM** Trust Model are considered to be "relying parties" (or trusted third parties). These relying parties do not necessarily need to be a subscriber of an **OGTM** certificate, but are requested to accept the "**OGTM** Relying Party agreement ", available at http://www.oiste.org/repository.

In the **OGTM** Trust Model, a particular Certification Policy could limit the right to be a relying party for a particular type of certificate, if this is the case, a specific Relying Party agreement" would be published.

1.3.5 Other participants

The **OGTM** Trust Model provides the following additional services to relying parties:

- Directory and Publication Services.
- Certificate Validation Services.
- Certificate Revocation Services.

OGTM reserves the right to delegate these services to third parties. These participants will follow an accreditation process defined by the **OGTM** and would be disclosed appropriately.

1.4 Certificate Usage

The OISTE Root CAs don't issue end-entity certificates. The detailed information on all the allowed certificate usages can be found in the different CP documents published by the OISTE PAA, to which the subordinate CAs are approved to adhere, and in the CPS published for these CAs.

1.4.1 Appropriate Certificate Uses

Certificate type	Description	Permitted uses
Issuing and Intermediate CA Certificate	Infrastructure certificate for all subordinate Certification Authorities operating in the trust models regulated by this CPS	Certificate Signing, CRL Signing
OCSP Certificate	Infrastructure certificate for Online Certificate Status Responders providing information on the subordinated CAs issued by the OISTE Roots	OCSP Response Signature

1.4.2 Prohibited certificate uses

In general, any usage that is not explicitly stated in section 1.4.1 of this document or the appropriate CP, is considered to be prohibited.

1.5 Policy Administration

1.5.1 Organization administering the document

This document is administered by the **OGTM Policy Approval Authority** (referred from now as **PAA**).

The **PAA** has a series of distinct functions but does not operate as a separate legal Entity. It is managed and organized in accordance with a process that draws on expertise within the OISTE Foundation. The **PAA** has been established to develop, review and/or approve the practices, policies and procedures for the entire Trust Model, subject to guidelines established by the members and advisors of the OISTE Foundation.

1.5.2 Contact Person (Contact Information)

Name	OISTE Foundation - OGTM Policy Approval Authority
email address	cps@oiste.org
Address	29, route de Pré-Bois - CP 853 CH-1215 Geneva 15 (Switzerland)

1.5.3 Person determining CPS suitability for the policy

The competent entity which determines the compliance and suitability of all CPS and the different supported CPs on behalf of the entire Trust Model is the **OGTM PAA**.

1.5.4 CPS approval procedures

The **OGTM PAA** defines and executes the procedures related to the approval of the CPS and CP and its subsequent amendments. Amendments will produce a new version of the document that will be published in the **OGTM** Policy Repository (specified in section 2.1 of this document).

The approval of major changes of documents related to the PKI, and specially for the CPS and CP, require a meeting of the PAA and the issuance of an approval memo signed by at least two members of the PAA. Minor versions only require the participation of a single member of the PAA in order to approve the publication of a new version.

It's required to issue new CP/CPS versions at least once a year. In the case of versioning conflict, the latest version that prevails is always the document published in the Policy Repository.

In the case of CPS published by CA adhered to the **OGTM,** the **OGTM PAA** will always validate and endorse the subordinate CPS, with the signature of at least one member of the **OGTM PAA**.

Once any document of the Trust Model (CPS or CP) is updated, the CAs must do a technical assessment to identify any possible impact and/or required configuration changes in the platforms.

1.6 Definitions and Acronyms

Definitions and Acronyms are included in Annex A (Glossary).

2 Publication and Repository Responsibilities

This section contains the provisions regarding the publication of policies, certificates and other public information needed for the participants to interoperate with the **OGTM**.

2.1 Repositories

The main repositories of the **OGTM** are:

- Policies repository for disclosure of CP, CPS and related information. This repository is a set of web pages and services available at the URL http://www.oiste.org/repository
- Certificate and Certificate Revocation information repositories. The Root CA certificates and Root Certificate Revocation Lists are published at the URL http://www.oiste.org/repository.

2.2 Publication

The **OGTM** is responsible for publication of information regarding practices, certificates, and the current status of certificates. Where appropriate, such responsibilities may be delegated to the Subordinate CAs operating under the OISTE Trust Model.

The shared repositories containing public information in the **OGTM** are managed by WISeKey SA or the operator of the Issuing CAs, and are available 24 hours a day, seven days a week. In the case of interruption by cause of "force majeure", the service will be re-established in the minimum possible time.

2.2.1 Statement on Compliance with CA/Browser Forum requirements

OISTE doesn't issue directly subscriber certificates affected by the CA/Browser Forum requirements, nevertheless, the Foundation expresses its commitment to ensure the compliance of the subordinate CAs with industry best practices and security controls. In particular, **OGTM** enforces regular review and compliance of the CP and CPS documents and practices with the latest version of the "Baseline Requirements" and "Extended Validation Requirements" for the scope to which these regulations apply (these requirements are available respectively at https://cabforum.org/baseline-requirements-documents/ and https://cabforum.org/extended-validation/)

In the case of discrepancy of any certification practices with the stipulations of the CAB/Forum requirements, it must be understood that those requirements must prevail to the CP and CPS documents.

2.3 Time or frequency of publication

The CPS and CP documents will be published every time they are modified, with a minimum review period of one year.

A certificate issued by any CA under the **OGTM** will be published immediately after its issuance.

In the case of revocation of a certificate, the appropriate CA will include this revocation information in the Certificate Revocation Lists (CRL) according to section 4.9.7 (CRL issuance frequency).

2.4 Access control on repositories

The **OGTM** makes its Repository publicly available in a read-only manner.

3 Identification and Authentication

The **OGTM** mandates the fulfilment of a set of required minimum controls that ensure the authenticity of the data included in certificates. These controls are enforced during the full lifecycle of certificates, certificate requests, and related documents. If non-validated attributes are allowed for a certain type of certificate, it will be explicitly indicated in the appropriate CP document and/or in the certificate itself.

This document reflects the common policies and controls for Identification and Authentication applied to the issuance of certificates for Subordinate CA.

It must be understood that the Identity Validation processes for end-entity certificates are stipulated in both the appropriate CP document and the CPS disclosed by the Subordinate CA issuing the certificate, therefore the reader must refer to those documents when evaluating end-entity certificates.

3.1 Naming

This section describes the elements regarding naming and identifying the subscribers of **OGTM** certificates.

3.1.1 Types of names

All subscribers are assigned a Distinguished Name (DN) according to the X.501 Standard. This DN is composed of a Common Name (CN), which includes a unique identification of the subscriber as described in section 3.1.4.2, and a structure of X.501 components as defined in section 3.1.4.

3.1.2 Need for names to be meaningful

All Distinguished Names must be meaningful, and the identification the attributes associated to the subscriber should be in a human readable form.

3.1.3 Anonymity of subscribers and pseudonyms

OGTM doesn't allow anonymity or pseudonyms in the certificates issued by the Roots.

Stipulations related to subscriber certificates are defined in the appropriate CP.

3.1.4 Rules for interpreting various name forms

The rules used in the **OGTM** to interpret the distinguished names of certificates issued under its Trust Model are defined by the ISO/IEC 9595 (X.500) Distinguished Name (DN) standard.

3.1.5 Uniqueness of names

OGTM requires uniqueness of names in the certificates issued by the Roots, except in the case of reissuances or renewals for the same entity.

Stipulations related to subscriber certificates are defined in the appropriate CP.

3.1.6 Recognition, authentication, and role of trademarks

The inclusion of a name in a certificate does not imply any right over that name, neither for the **OGTM** nor the applicant, nor the subscriber. The **OGTM** reserves the right to refuse a certificate request, or revoke an existing one, if a conflict is detected over ownership or copyright of a name.

In any event, the **OGTM** will not attempt to intermediate nor resolve conflicts regarding ownership of names or trademarks.

3.2 Initial Identity Validation

OGTM performs "face to face" identity validation for the certificates issued by the Roots. Stipulations related to subscriber certificates are defined in the appropriate CP.

In general, any Issuing CA operating in the OGTM and issuing SSL/TLS certificates, must ensure compliance with the baseline requirements and extended validation guidelines mandated by the CA/Browser Forum, by adequately implementing the stipulations found in the CP for SSL/TLS Certificates. The issuing CA will disclose adequately this implementation in its own CPS.

3.2.1 Method to prove possession of private key

OGTM requires the usage of digital signatures, using the private key, in certificate signing requests processed by the Roots.

Stipulations related to subscriber certificates are defined in the appropriate CP.

3.2.2 Authentication of organization identity

Before issuing a certificate for a subordinate Certification Authority **OGTM** requires the fulfillment of a legally binding agreement between the organization and the OISTE Foundation, which includes the appropriate validation of the organization identity and signatories of the agreement.

Stipulations related to subscriber certificates are defined in the appropriate CP.

3.2.3 Authentication of individual identity

OGTM doesn't allow the issuance of subordinate CAs to individuals or natural persons. For the persons involved in the CA Key Ceremonies, it's requires to prove their identity via government-issued identity documents, and their authorization to participate in the issuance process.

Stipulations related to subscriber certificates are defined in the appropriate CP.

3.2.4 Non-verified subscriber information

OGTM doesn't allow to include non-verified identity-related information in any certificate issued by a certification authority operating in the trust model.

Additional stipulations related to subscriber certificates can be defined in the appropriate CP.

3.2.5 Validation of authority

OGTM requires that any person participating in any operating process related to certificate generation or status modification is explicitly authorized.

Stipulations related to subscriber certificates are defined in the appropriate CP.

3.2.6 Criteria for interoperation

A Certification Authority that wishes to interoperate with the **OGTM** is required to undergo an internal accreditation process to ensure the compliance with this CPS.

If this accreditation process is successful, it will result in the creation of an "Issuing CA" under the **OGTM** that adheres to this CPS and authorized to issue certain Certificate Policies.

3.3 Identification and Authentication for Re-key Requests

This section addresses the following elements for the identification and authentication procedures for re-key for each subject type (CA, RA, subscriber, and other participants). Unless otherwise specified, it can considered as equivalent the activities linked to "re-key" (new certificate for an existing subscriber, using a new key pair) and "renewal" (new certificate for an existing subscriber, using the same key pair).

In general, these elements are stipulated in the appropriate CP.

3.3.1 Identification and authentication for routine re-key

For CA Certificates, **OGTM** requires that all re-keying is treated as a new CA Key Ceremony, following the same procedures indicated in the above sections.

Additional stipulations related to subscriber certificates can be defined in the appropriate CP.

3.3.2 Identification and authentication for re-key after revocation

The **OGTM** does not support re-key of certificates after revocation. The subscriber must apply for a new digital certificate by using the same procedures as for its issuance.

3.4 Identification and Authentication for Revocation Requests

The Identification Policy for revocation requests is, generally, the same as stipulated for initial registration. The preferred method to authenticate revocation requests is an authentication based in a digital certificate owned by the certificate subscriber, or authorized party. Password-based authentication may be accepted in certain cases.

4 Certificate Life-Cycle Operational Requirements

The stipulations included in this section are understood as common for all the certificates issued under the **OGTM** Root, unless otherwise specified in this document.

It must be noted that, where applicable, CAs operating under the OGTM must respect the requirements set by the CA/Browser Forum Baseline and EV Requirements, adding the necessary stipulations in their disclosed CPS.

4.1 Certificate Application

For CA Certificates, before issuing a new certificate for a subordinate Certification Authority **OGTM** requires the fulfillment of a legally binding agreement between the affiliated organization and the OISTE Foundation, which includes the appropriate validation of the organization identity and signatories of the agreement. Additionally, for each Subordinate CA, it's required the fulfillment of a "CA Naming Request", which must be signed by authorized representative of the affiliate.

For subscriber certificates, the Registration Authorities operating under the **OGTM** are competent and responsible for determining if the type of the requested certificate is adequate for the applicant and future subscriber, in conformity with the Certificate Policy related to that certificate, and therefore to proceed or not with the certificate application. The Certificate Application process must include a mean to express acceptance with the Subscriber Agreement, by means of a manuscript signature or another valid mechanism, and it's a first step to begin the certificate issuance process.

4.1.1 Who can submit a certificate application

A certificate application can be submitted by the subject of the certificate or by an authorized representative of the subject.

4.1.2 Enrolment process and responsibilities

OGTM requires that any person participating in any process related to the life cycle of certificates for subordinate CAs is explicitly authorized, being deemed responsible of the dutiful execution of its responsibilities in the CA Ceremony process.

Stipulations related to subscriber certificates are defined in the appropriate CP.

4.2 Certificate Application Processing

This section describes the procedures for processing certificate applications in the **OGTM** Trust Model.

4.2.1 Performing identification and authentication functions

Before issuing a certificate from an OISTE Root for a subordinate Certification Authority, it's required that two representatives of the PAA identify the CA Naming Application and rightfulness to operate a subordinate CA under the OISTE Root.

*The identification and authentication functions for subscriber certificates are delegated to the Registration Authorities operating under the **OGTM**, and stipulated in the CPS of the subordinate CA.*

4.2.2 Approval or rejection of certificate applications

An approval of a certificate application derives from the execution of the certificate issuance procedures, as defined in the section 4.3 of the CPS and the appropriate Certificate Policy.

A rejection of a certificate application results in a notification being sent to the applicant by appropriate means and is registered for further reference.

4.2.3 Time to process certificate applications

There is no time limit stipulated to complete the processing of an application.

4.3 Certificate Issuance

An approved certificate request will be processed by the authorized responsible.

4.3.1 CA actions during certificate issuance

A Certification Authority adhering to the **OGTM** proceeds with the issuance of a certificate only after executing the necessary measures to verify that the signing request is authorized and genuine, as per the particular controls are stipulated in the CPS and/or appropriate Certificate Policy.

4.3.2 Notifications to subscriber by the CA of issuance of certificate

For CA Certificates, **OGTM** notifies directly to the authorized CA responsible.

Stipulations related to subscriber certificates are defined in the appropriate CP.

4.4 Certificate Acceptance

Certificate acceptance is the final step in the certification issuance process. After Acceptance the certificate owner is entitled to use the certificate and issue valid digital signatures.

4.4.1 Conduct constituting certificate acceptance

For CA Certificates the CA representative must acknowledge the reception of the certificate, verifying that the Key Fingerprint matches the request. Installing the CA Certificate in the CA server constitutes tacit acceptance.

Stipulations related to subscriber certificates are defined in the CPS published by the Issuing CA.

4.4.2 Publication of the certificate by the CA

The CAs operating under the **OGTM** publish all issued certificates as specified in section 2 of this document.

4.4.3 Notification of certificate issuance by the CA to other entities

The CA only notifies the Registration Authority from which it received the request of the issuance of a certificate. It is the RA's duty to notify the certificate subscriber, as stipulated in section 4.3.2 of the appropriate CP.

4.5 Key Pair and Certificate Usage

The certificates issued by the **OGTM** are used to provide authenticity, integrity, confidentiality and/or non-repudiation in electronic transactions and other computerized functions.

4.5.1 Subscriber private key and certificate usage

For CA Certificates the private key may only be used according to the CPS published by the subordinate CA, subject to approval by the **OGTM** PAA.

Stipulations related to subscriber certificates are defined in the appropriate CP.

4.5.2 Relying party public key and certificate usage

Relying parties must access and use the public key and certificates issued under the **OGTM** as stipulated in this CPS and as indicated in the "Relying Party Agreement" document, made public at the web page http://www.oiste.org/repository.

4.6 Certificate Renewal

Certificate Renewal is understood as the issuance of a new certificate to a subscriber who maintains the key pair generated for the original certificate. Certificate renewal may not be supported depending on the appropriate CP.

4.6.1 Circumstance for certificate renewal

For CA Certificates it is allowed the certificate renewal for these purposes:

- Extend the validity period
- Modify the name constraints, enhanced key usages or other non-identity extensions

Stipulations related to subscriber certificates are defined in the appropriate CP.

4.6.2 Who may request renewal

The certificate renewal can be requested by the same entities allowed to request the first issuance of the certificate.

4.6.3 Processing certificate renewal requests

Certificate renewal requests are processed according to the same rules than the initial issuance.

4.6.4 Notification of new certificate issuance to subscriber

The notification of the issuance of a renewed certificate it will occur as described in section 4.3.2 of this document.

4.6.5 Conduct constituting acceptance of a renewal certificate

As stipulated in section 4.4.1 of this document.

4.6.6 Publication of the renewal certificate by the CA

The CAs operating under the **OGTM** publish all issued certificates as specified in section 2 of this document.

4.6.7 Notification of certificate issuance by the CA to other entities

The CA only notifies the Registration Authority from which it received the request of the issuance of a certificate. It is the RA's duty to notify the certificate subscriber, as stipulated in section 4.3.2 of the appropriate CP.

4.7 Certificate Re-key

Certificate Re-Key is understood as the issuance of a new certificate to a subscriber that also generates a new key pair. This process is supported for all certificate types.

4.7.1 Circumstance for certificate re-key

Any certificate that is not revoked can be re-keyed.

4.7.2 Who may request certification of a new public key

The certificate renewal can be requested by the same entities allowed to request the first issuance of the certificate.

4.7.3 Processing certificate re-keying requests

Certificate re-key requests are processed according to the same rules than the initial issuance.

4.7.4 Notification of new certificate issuance to subscriber

The notification of the issuance of a new certificate it will occur as described in section 4.3.2 of this document.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As stipulated in section 4.4.1 of this document.

4.7.6 Publication of the re-keyed certificate by the CA

The CAs operating under the **OGTM** publish all issued certificates as specified in section 2 of this document.

4.7.7 Notification of certificate issuance by the CA to other entities

The CA only notifies the Registration Authority from which it received the request of the issuance of a certificate. It is the RA's duty to notify the certificate subscriber, as stipulated in section 4.3.2 of the appropriate CP.

4.8 Certificate Modification

The **OGTM** does not allow the modification of certificates during their validity period. If the information contained in a certificate ceases to be valid, or the circumstances of the subscriber change in such a manner that the conditions expressed in the CPS or the CP are not met, then the only accepted procedure is the revocation and reissuance of a new certificate.

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate Revocation and Suspension

All Certification Authorities operating under the **OGTM** ensure, by establishing the necessary means, that a certificate that compromises the Trust Model for any reason is prevented from being used by either revoking or suspending that certificate.

Suspension of certificates is only supported for personal and device certificates, and explicitly disallowed for SSL certificates, according to the CA/Browser Forum requirements, and therefore is disallowed for any certificate existing under an OISTE Root which is approved to issue publicly trusted SSL certificates.

4.9.1 Circumstances for revocation

Any Certification Authority operating under the OGTM must assume the stipulations contained in this section.

4.9.1.1 Reasons for Revoking a Subscriber Certificate

A Certification Authority operating under the **OGTM** must revoke within 24 hours a certificate that it has issued upon the occurrence of any of the following events:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate; or
5. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

A Certification Authority operating under the **OGTM** must revoke within 5 days a certificate that it has issued upon the occurrence of any of the following events:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of this CPS or appropriate CP;
2. The CA obtains evidence that the Certificate was misused;
3. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address 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. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. The CA is made aware of a material change in the information contained in the Certificate;
7. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
8. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
9. The 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 CA's Certificate Policy and/or Certification Practice Statement; or
11. The CA 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, or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Revocation of SSL Certificates, in particular, will be processed as defined by the requirements published by the CA/Browser Forum, as appropriate.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

An issuing Certification Authority operating under the **OWGTM** will be revoked within 7 days upon the occurrence of any of the following events:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;

7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.

4.9.2 Who can request revocation

The certificate subscriber or its legal representative can request the revocation of an individual or organizational certificate.

Third parties may request certificate revocation for problems related to fraud, misuse, or compromise. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

4.9.3 Procedure for revocation request

The procedure to request the revocation of a Subordinate CA of the OISTE Roots, is to contact the Foundation via e-mail message to cps@oiste.org, or the contact details disclosed in section

To report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, the main and preferred method is sending an e-mail message to cps@oiste.org.

The procedure to be used for end-entity certificate revocation requests is must be published by the Issuing CA in its own CPS and communicated to the subscriber during the issuance process.

The common practice for all certificates issued under the **OGTM** Trust Model is for revocation requests to be accepted automatically and produce an immediate revocation in the case of:

- Remote requests sent by e-mail or via a web page or service, appropriately authenticated by the subscriber or its representative.
- Face-to-face requests addressed to an official Registration Authority representative and the identity of the requestor is proved by the same means as used for certificate registration.
- Revocation requests sent by an official Registration or Certification representative operating under the **OGTM** Trust Model.

Except for SSL certificate which don't allow suspension, revocation requests communicated by other means (i.e. by non-signed electronic messages or by telephone) which do not unequivocally authenticate the requestor can produce a temporary suspension of the certificate, as defined in sections 0 to 4.9.16.

4.9.4 Revocation request grace period

There is no stipulation for grace periods for revocation requests. The revocation process will be started immediately upon the receipt of such a request by an authorized party.

4.9.5 Time within which CA must process the revocation request

Revocation requests are processed by the CA within the shortest possible period, and always in accordance to the limits set in section 4.9.1.

4.9.6 Revocation checking requirement for relying parties

The **OGTM** requires that all parties willing to rely on certificates issued under the Trust Model check the status of these Certificates on each digital signature verification and authentication request using the certificate. This requirement can be fulfilled by consulting the most recent CRL from the CA that issued the Certificate or by using the **OGTM Online Certificate Status Protocol Server** (OCSP).

The information necessary to locate these revocation services is included in all **OGTM** certificates, using the standard CDP and/or AIA extensions.

4.9.7 CRL issuance frequency

The **OGTM Root CAs** issue a full CRL every year, with a typical overlapping period of one week. This CRL will contain the revoked, if any, certificates for **OGTM** Policy CAs or Issuing CAs, as appropriate for the hierarchy. New CRLs are published immediately if a new subordinated CA is revoked.

The CRL issuance frequency for Subordinate Certification Authorities is stipulated in the CPS published by the appropriate CA. For the specific case of SSL and Code Signing certificates, the **OGTM** will ensure the compliance of the Baseline (and Extended Validation, for EV certificates) Requirements of the CA/Browser Forum.

4.9.8 Maximum latency for CRLs

CRLs are posted to their distribution point within the minimum possible time after generation.

4.9.9 On-line revocation/status checking availability

The Certificate Authorities operating in the **OGTM** can provide an OCSP service that is typically available on a 24x7 basis. The OCSP service availability is stipulated by the subordinate CAs in their CPS.

In particular for SSL and Code Signing certificates, **OGTM** will ensure compliance with the applicable Baseline and/or Extended Validation requirements from the CA/Browser Forum.

4.9.10 On-line revocation checking requirements

On-line revocation checking is openly provided without restriction to all Participants in the PKI, for the certificate types that include the appropriate AIA extension.

Relying parties are requested to always check the validity of the certificate on which they rely, as stipulated in section 0.

4.9.11 Other forms of revocation advertisements available

No stipulations.

4.9.12 Special requirements regarding key compromise

Any party detecting a key compromise at any level in the **OGTM** Trust Model is requested to immediately communicate it to a Registration or Certification Authority.

In particular for SSL certificates, but applicable for any other certificate type issued, it's also requested to Subscribers, Relying Parties, Application Software Vendors and other third parties to report any potential issue to the Certification Authority (Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates).

The appropriate methods to demonstrate key compromise are:

- Create and sign a text file,
- Create a custom CSR file, and/or
- Send the private key, or a link to where it's publicly disclosed.

The main method for these communications is the stipulated in section 4.9.3.

4.9.13 Circumstances for suspension

Suspension is not allowed for SSL or CA Certificates. Please refer to the appropriate Certificate Policy for other specific stipulations on subscriber certificates.

4.9.14 Who can request suspension

Same as 4.9.2.

4.9.15 Procedure for suspension request

Same as 4.9.3.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate Status Services

Any CA operating in the **OGTM** must provide a highly available and reliable service for checking the status of all certificates issued under its Trust Model. In particular, CAs being able to issue SSL certificates are bound to comply with the CABF Baseline Requirements.

4.10.1 Operational characteristics

Certificate Status Services are accessible through HTTP servers owned by the **OGTM** Certification Authorities. The Services can be accessed by downloading revocation lists (CRL) or by sending requests to OCSP servers.

The appropriate certificate revocation information service URLs are included in standard extensions within the issued certificates.

4.10.2 Service availability

The Certificate Status Services are available on a 24x7 basis.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

"End of Subscription" is understood to occur after the expiration or revocation of a certificate, and it is unique for that particular certificate, not affecting additional subscriptions (if any) that the end entity may hold within the **OGTM**.

4.12 Key Escrow and Recovery

For infrastructure certificates, as CA, RA or others, appropriate back-up policies must be implemented, according to section 6.2.4

Key Escrow for end-entity certificates is stipulated in the appropriate CP.

4.12.1 Key escrow and recovery policy and practices

As stipulated in the appropriate CP.

4.12.2 Session key encapsulation and recovery policy and practices

As stipulated in the appropriate CP.

5 Management, Operational, and Physical Controls

This section describes the non-technical security controls used by the participants[2] involved in the issuance, publishing and management of keys within the **OGTM**. The **OGTM** asserts the importance of these controls as a fundamental basis to provide trust to subscribers and all relying parties, and therefore establishes and maintains the necessary means to ensure and demonstrate that these controls are enforced.

These controls are under surveillance and audited both internally and externally by accredited bodies. The public manifests of these audits are published on a regular basis in the **OGTM** web site (http://www.oiste.org/repository).

The **OGTM** allows third parties to host and operate[3] some of the components of its infrastructure. If such a delegation occurs, the assigned party will be requested to meet the controls stipulated in this section and an auditing process will be executed to ensure that the necessary measures to ensure these controls are effective are in place and enforced.

In particular:

- The OISTE Foundation delegates the hosting and operations of the "Root CA" and the "Policy CAs" (and related certificate publication and verification services) to WISeKey.
- The "Issuing CAs" (and related certificate publication and verification services) are hosted and operated by their respective owners. These participants are allowed to delegate the hosting and operation to WISeKey only; other delegations or outsourcing are only permitted after a security assessment and a formal authorization.
- Registration Authorities and Registration Authority Points are appointed by the CA Operator. Registration Authorities are not allowed to delegate their operations to other parties.

5.1 Physical Security Controls

This section describes the physical controls on facilities housing **OGTM** components.

5.1.1 Site location and construction

The **OGTM** information systems are located in Secure Datacenters providing adequate security levels and under surveillance 24 hours a day, 7 days a week. These Datacenters are built in such a manner that relevant critical physical risks are managed.

5.1.2 Physical access

The **OGTM** Secure Datacenter implements diverse nested security perimeters. The access from an outer to an inner perimeter requires different security and authorization controls. Among these controls, biometric door access, video surveillance and intrusion detection systems are implemented.

[2] The security requirements for subscribers and relying parties are described in their particular agreements. These agreements could stipulate different controls depending on the Certificate Policy and they are published by the Issuing CA as disclosed in its CPS.

[3] Critical operations are not allowed to be outsourced. In particular, Key Ceremonies are not allowed to be delegated in any case, and must always be executed by the Certification Authority issuing the subordinated CA's Certificate.

5.1.3 Power and air conditioning

The **OGTM** Secure Datacenter implements power and air conditioning systems sufficiently dimensioned to accommodate the operating needs.

5.1.4 Water exposures

The facilities are located in a place where natural flooding risks are controlled, and they are equipped with flooding sensors and alarms.

5.1.5 Fire prevention and protection

The facilities implement fire detection, prevention and protection controls.

5.1.6 Media storage

Sensible information media are stored securely in fireproof containers and high security safes, depending on the media type and the classification of the information they contain.

These containers and safes are located in redundant placements, in order to eliminate the risks of using a single location (i.e. in the case of fire or water damage).

Access to these storage locations and items is restricted to authorized persons and regulated by security procedures.

5.1.7 Waste disposal

The disposal of optical or magnetic media and paper containing any information generated during **OGTM** operations is executed following procedures established for such purposes, including demagnetization and/or destruction processes, depending on the media type to be disposed.

5.1.8 Backup

OGTM executes a backup copy of all information needed to promote a secondary datacenter to operational status in the event of a disaster preventing the main datacenter from maintaining an adequate service level.

A remote backup copy is periodically made and stored in a way such that dual access control is required to restore the backup copies.

5.2 Procedural Controls

The information systems and services incorporated in the **OGTM** are operated in a secure manner, following a set of predefined procedures that are enforced by the **OGTM** and verified through periodical auditing activities.

For security reasons the information related to these controls are classified as “CONFIDENTIAL” and this document may only disclose a summarized version. Further detailed information is only disclosed to accredited auditors who are responsible for reviewing **OGTM** components and operations.

5.2.1 Trusted roles

The **OGTM** establishes and enforces a strict security policy to control all operations performed at any level of the Trust Model. This includes the identification and control of the Persons performing those operations. These Persons are considered “Trusted Roles” and include, but are not limited to:

- Certification Authority Manager
- Certification Authority Administrator
- Certification Authority Operator
- Registration Authority Manager
- Registration Authority Administrator
- Registration Authority Operator
- Support, Training and Communication Manager
- Legal Advisor
- Documentation Manager
- Systems Administrator
- Security Manager
- Security Administrator and Operator
- Policy Approval Authority Member

Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS (section 5.3).

5.2.2 Number of persons required per task

The **OGTM** establishes the need for the segregation of duties based on job responsibility in order to ensure that the adequate number of Trusted Persons is required to perform sensitive tasks.

The roles requiring separation of duties is stipulated in section 5.2.4.

5.2.3 Identification and authentication for each role

All the persons assuming a role in the **OGTM** systems[4] follow an authorization process that entitles them to access the appropriate information and systems for their role.

Physical access control for all the authorized persons accessing **OGTM's** systems and services systems is typically enforced using two factor authentication that usually includes biometrics.

5.2.4 Roles requiring separation of duties

Roles requiring Separation of duties include at least the following:

- Any activity involved in the operation of a Root Certification Authority.
- Enabling a CA into a production status (CA Ceremony procedures)
- Issuance, or revocation of CA Certificates
- Validation of information and issuance of high assurance subscriber certificates (i.e. EV SSL Certificates)

5.3 Personnel Security Controls

Personnel bearing one of the roles defined in section 5.2.1 will be required to fulfil the "**OGTM Trusted Professional Policy**", summarized in the following sections.

[4]See note 2

5.3.1 Qualifications, experience, and clearance requirements

Personnel acting directly or indirectly for the **OGTM** will be required to possess the required qualification and/or proved experience in certification service provision environments. All involved personnel will be required to act according to the **OGTM** Security Policy and to possess:

- Knowledge and training (according to the role assigned to the person) in Public Key Infrastructures.
- Knowledge and training (according to the role) in Information Systems Security.
- Knowledge and training specific for the responsibilities assigned.

5.3.2 Background check procedures

The Human Resource Department conducts verification checks on permanent staff at the time of job applications, and ensures that all personnel with access to sensitive information are trustworthy and understand their responsibilities; this includes at a minimum the following:

- Availability and verification of satisfactory references;
- Confirmation of claimed academic and professional qualifications;
- Identity checks of passport or similar document.

5.3.3 Training requirements

Personnel directly involved in **OGTM**, including "Issuing CAs" operated by third parties and Registration Authorities, will follow an internal training plan adapted to their assigned attributions. This training will be compliant with industry regulations, as the CA/Browser Forum Baseline and/or Extended Validation Requirements, as applicable.

5.3.4 Retraining frequency and requirements

Retraining sessions are required for all involved personnel in the case of environmental, technology and/or operative changes. Changes in practices and/or policies are communicated to all involved personnel.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

If an unauthorized action is detected the **OGTM** will undertake necessary disciplinary actions. Any action that (intentionally or unintentionally) contravenes the Certification Practice Statement.

Upon detection of an unauthorized action the **OGTM** will initiate an investigation process. During this process the involved persons will be prevented from obtaining access to **OGTM** systems and information.

Disciplinary actions will be taken after the investigation determines the severity and intent of the action.

5.3.7 Independent contractor requirements

External contractors are required to agree with the Information Security policies of the **OGTM** and temporary staff not already covered by an existing confidentiality agreement shall also be required to sign the Non-Disclosure Agreement prior to being granted access to Information resources.

The agreement is reviewed when there are changes to employment terms or contracts.

5.3.8 Documentation supplied to personnel

All personnel incorporated within the **OGTM** are provided access to at least the following information:

- Certification Practices Statement
- Certificate Policies
- Privacy Policy
- Security Policy
- Organization chart and assigned functions and responsibilities
- Operational procedures
- Incident response procedures

5.3.9 Contract termination and assigned role change procedures

In the event that a contract is terminated, or the role assigned to a person is changed, **OGTM** ensures that the appropriate procedure is executed. This procedure includes at least the necessary changes in the privileges granted to access facilities, information systems and documentation.

Assigned material (smart cards, computers, etc.) will be returned or reassigned as necessary.

The change or termination will be notified to all involved parties.

5.4 Audit Logging Procedures

This section describes the event logging and audit systems that have been implemented to maintain a secure environment in the **OGTM**.

5.4.1 Types of events recorded

OGTM records in their servers all events related to:

- CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction as captured by procedure documentation; and
    b. Cryptographic device lifecycle management events as captured by procedure documentation.
- CA and Subscriber Certificate lifecycle management events, limited to:
    a. Certificate requests and revocation as captured by CA logs;
    b. Verification activities
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls as captured by registration officers;
    d. Acceptance and rejection of certificate requests as captured by CA logs;
    e. Issuance of Certificates as captured by CA logs
    f. Generation of Certificate Revocation Lists as may be captured by CA logs (NB CRLs are not retained, only the record of its generation)
    g. Generation of OCSP entries as may be captured by available OCSP server logs (NB OCSP entries are not retained, only the record of their generation if recorded by the OCSP server)
- Security events, including:
    a. Successful and unsuccessful PKI system access attempts as captured by operating system logs;
    b. Major PKI and security system actions performed as captured by operational logs;

c. Security profile changes as captured by operating system logs;
d. System crashes, hardware failures, and other anomalies in server logs;
e. Firewall and router activities as captured by device logs; and
f. Entries to and exits from the CA facility as captured by access control logs.

5.4.2 Frequency of processing log

Logs are processed and audited when required.

For systems that are kept offline, as the Root CA, audit logs are only reviewed when an operation is executed.

5.4.3 Retention period for audit log

OGTM and involved parties retain all audit logs as specified in section 5.5.2.

5.4.4 Protection of audit log

All audit records and archives are stored in fireproof cabinets only accessible for authorized persons.

The destruction of an audit record can only executed after signed authorization from the **OGTM** auditor and the **OGTM** Information Security Manager. A trace of the destructed materials is kept for future references.

5.4.5 Audit log backup procedures

The audit logs are backed up using incremental and remote procedures.

5.4.6 Audit collection system (internal vs. external)

The collection systems for audit logs in **OGTM** is a combination of automatic and manual processes, and is executed by the appropriate operating systems, software applications, and personnel operating these systems.

5.4.7 Notification to event-causing subject

No stipulations.

5.4.8 Vulnerability assessments

OGTM executes regular vulnerability assessment by monitoring the activity logs, at least according to the minimum frequencies mandated by the CAB/Forum. In depth assessments and checks are performed on a yearly basis, including conformance to disaster recovery plans. In the event that an assessment could not be performed or was delayed, the **OGTM** will inform the involved parties and records of such an event and its cause will be kept for future reference.

This security analysis implies the identification of necessary tasks to correct detected vulnerabilities.

5.5 Records Archival

This section includes the stipulations regarding record retention policies.

5.5.1 Types of records archived

The information and events archived are:

- Information generated (at CA and RA) during the life cycle of all **OGTM** certificates,
- Contracts and agreements,
- Audit logs stipulated in section 5.4 of this CPS.

5.5.2 Retention period for archive

Archived records and audit logs are kept Records are retained for at least the validity of the involved certificates.

For the particular case of SSL and EV certificates, The CA must ensure the retention period of seven years stipulated by the CAB Forum in its guidelines.

5.5.3 Protection of archive

Access to archived materials is restricted to authorized persons, and controls to ensure the archive integrity are enforced.

5.5.4 Archive backup procedures

Daily backup copies are executed. The main copy is kept in the principal **OGTM** facility and stored inside a secured zone. Copies are periodically stored offsite.

5.5.5 Requirements for time-stamping of records

In addition to stipulations in 5.5.3, a time stamp is included in the digitally signed records. The time stamp needs not be of cryptographic nature.

5.5.6 Archive collection system (internal or external)

Archive collection is an internal task in the **OGTM** that cannot be outsourced to third parties.

The only exception are authorized Registration Authority points, which are allowed to archive information collected during the certificate life-cycle. In such case, this information must be kept securely, accessible only for authorized persons, and made available to any internal or external auditing entity mandated by **OGTM**.

5.5.7 Procedures to obtain and verify archive information

Only authorized personnel obtain access to the physical media containing archives, backups and other recorded information.

Integrity checks are performed automatically if the archive includes a digital signature.

5.6 Key Changeover

OGTM requires the creation of new keys for a CA needing to renew its certificate. Only in exceptional cases it can be accepted to repeat a CA Creation Ceremony maintaining the same keys created in a Hardware Security Module for a previous ceremony, in order to amend any error in the process.

When creating a new certificate for an entity, the validity period applied to this certificate will be constrained to the validity of the keys of the Certification Authority issuing it.

5.7 Compromise and Disaster Recovery

In the event that **OGTM** systems and services are not available for a period greater than 12 hours, the Continuity Plan will be activated. This Continuity Plan seeks to ensure that the critical services (as stated in section 5.7.4) are available in less than 72 hours after the plan is activated.

The following sections summarize specific situations and the stipulated reaction in **OGTM**. The detailed Continuity Plan is a confidential document.

5.7.1 Incident and compromise handling procedures

The Certification and/or Registration Authorities operating under the **OGTM** are required to enforce the necessary controls to ensure and demonstrate that the Incident and Compromise Handling Procedures are effective. Involved people must be conveniently trained in their roles and responsibilities in the execution of their duties.

The following subsections disclose the procedures executed in such these events.

5.7.2 Computing resources, software, and/or data are corrupted

If the hardware or software resources are altered or suspected to have been altered, the **OGTM** will stop normal operations until a secure environment is established. In parallel, an audit will be conducted in order to identify the cause and stipulate the necessary actions to avoid future iterations.

In the event digital certificates are issued during the uncertainty period and a risk exists that these certificates could be compromised, then those certificates will be revoked and subscribers will be notified of the need to reissue their certificates.

5.7.3 Entity private key compromise procedures

In the case a private key is compromised in the **OGTM** architecture and in addition to stipulations in section 5.7.2, the subordinated entities depending on the compromised private key will be notified of this event and the necessary actions will be undertaken.

All certificates issued by entities subordinated to the compromised key from the time of the key's compromise and the certificate's revocation will be revoked, and the involved parties notified as stipulated in this CPS. Additional steps to re-issue the necessary certificates will be taken.

5.7.4 Business continuity capabilities after a disaster

In the event of a disaster (independently of its nature) that affects **OGTM's** main facilities, and any services that are provided from these, the **OGTM** Service Continuity Plan will be activated, ensuring that the services identified as "Critical" are available in less than 72 hours after the Plan activation. The rest of services would be available in the reasonable terms, as judged adequate for their importance and criticality level.

5.8 CA or RA Termination

The causes that could imply the termination of a Certification or Registration Authority operating under the **OGTM** are:

- Private Key Compromise
- A political or judicial decision
- A Contract Termination after a breach of the corresponding Terms and Conditions

In the case a Certification Authority under **OGTM** is forced to terminate its activities, the minimum actions to be executed are:

- Immediately after there's a Termination decision, notify all certificate subscribers
- Revoke all certificates under the CA.
- Inform all relying parties that have a registered direct relationship with that Certification Authority about the termination of the certificate service provision. This will also terminate the accreditation granted to the Certification Authority to operate under **OGTM**.
- Publish a public notice of the termination within the repository section of the affected CA's web site, and undertake other public communications as deemed necessary to inform the wider relying party community.

In the case an **OGTM Root Certification Authority** is terminated, this will imply the termination of the entire hierarchy dependent of that Root CA.

6 Technical Security Controls

This section describes the measures taken by Certification Authorities operating under the **OGTM**[5]. The **OGTM** believes these controls are fundamental to provide trust to subscribers and all relying parties, and has therefore established the necessary means to ensure and demonstrate that these controls are enforced. These controls are under surveillance and audited both internally and externally by accredited bodies. The public manifests of these audits are published on a regular basis in the web site (http://www.oiste.org/repository).

6.1 Key Pair Generation and Installation

Under the **OGTM**, Key Pairs are generated under the necessary security levels and always occurring in secure physical facilities and under the adequate personnel control.

6.1.1 Key pair generation

Key Pairs of Certification Authorities operating in the **OGTM** are generated and installed under a procedure compliant with applicable regulations. Main details of this procedure are:

- The Root Certification Authority key creation ceremony is audited by an external qualified auditor[6].
- Subordinated Certification Authorities are generated under direct supervision of internal auditors from WISeKey.
- CA Ceremonies are executed by designated trusted personnel.
- There's a pre-defined execution script that must be followed during the Ceremony.
- During the Ceremony, enough audit track is recorded in order to proof that the Ceremony was executed as planned and without any security risk.
- After the Ceremony, a Ceremony Report is generated and properly archived for future reference.

Key pairs for the Root Certification Authorities in the **OGTM** are generated in hardware security modules (HSM) accredited under the standards specified in section 6.2.1.

Key pairs for the Policy and Issuing Certification Authorities in the **OGTM** may be generated in hardware security modules (HSM) accredited under the standards specified in section 6.2.1.

Key pairs for the Policy and Issuing Certification Authorities in the **OGTM** may be generated in escrowable form and protected as required under WebTrust requirements, and imported and operated within hardware security modules (HSM) under the standards specified in section 6.2.1.

Other Key Pairs than the ones assigned to Certification Authorities can be generated by software components, except the "CertifyID URA Admin" certificates, which must be generated in Secure Signature Devices (FIPS 140-1 Level 2 and equivalents, or higher).

For Subscriber Certificates, the key generation must occur as stipulated in the appropriate CP.

6.1.2 Private key delivery to subscriber

It is not allowed the manipulation of private keys corresponding to CA certificates.

Stipulations related to subscriber certificates are defined in the CPS published by the Issuing CA.

[5]See note 2 and Introduction for section 5. These controls are defined for all Certification Authorities under **OWGTM**.
[6] This applies for any Root CA incorporated to the Trust Model after the year 2007.

6.1.3 Public key delivery to certificate issuer

It is not allowed the generation of key pairs corresponding to CA certificates.

Stipulations related to subscriber certificates are defined in the CPS published by the Issuing CA.

6.1.4 CA public key delivery to relying parties

The public keys of all Certification Authorities operating under the **OGTM** Trust Model are included in the corresponding certificate and published and can be freely downloaded from its repository which is located at http://www.oiste.org/repository.

Trusted Root Certificates may be obtained directly from the appropriate repositories in most browsers and operating systems.

6.1.5 Key sizes

The **OGTM** enforces the use of minimum length 2048-bit RSA and ECC NIST P-256, P-384 for key pairs at all levels of the hierarchy.

Hashing algorithms supported are SHA-1 and SHA-2, depending on the hierarchy to which the end-entity certificate belongs, as described in 1.3.1. In particular, no issuance of new SHA-1 SSL or CA certificates after 31-December-2015.

6.1.6 Public key parameters generation and quality checking

The algorithm used in the **OGTM** for key generation is RSA or ECC.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Key usage purposes for CA certificates is restricted to digital signature, CRL signature and certificate signing.

Stipulations related to subscriber certificates are defined in the appropriate CP.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The **OGTM** has established controls to ensure that the risks derived from a private key compromise are managed and kept under reasonable levels. These controls are different for the main components (Certification Authorities) and end subscriber keys.

6.2.1 Cryptographic module standards and controls

Certification Authorities in the **OGTM** are required to use Hardware Security Modules, at least compliant with FIPS 140-2 Level 2 for PKI components (Level 3 for CA components).

Requirements for End-User cryptographic devices (if any) can vary in terms of the expected assurance level and detailed in the appropriate CP document.

6.2.2 Private key (n out of m) multi-person control

Private keys for Certification Authorities are always under multi-person control. Activation data needed to enable a Certification Authority will be shared in such a way that at least two authorized persons are needed to perform any sensitive operation on a Certification Authority, except where unattended operational restart of Issuing CAs is enabled.

Private keys for end-entities are under the sole control of the subscriber or authorized representative.

6.2.3 Private key escrow

Private key escrow is only provided for end-user personal certificates, as described in previous sections.

6.2.4 Private key backup

Backup copies of CA private keys for all Certification Authorities under the **OGTM** Trust Model are kept for routine recovery and disaster recovery purposes. Such keys are always stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of this CPS.

Private key backup for end-user subscribers, if supported for a certain certificate type, it would be implemented as described in the appropriate CP.

6.2.5 Private key archival

The CA shall not provide key archival services.

6.2.6 Private key transfer into or from a cryptographic module

For Certification Authorities operating under the **OGTM** Trust Model it is mandatory that key pairs are operated in Hardware Security Modules as defined in section 6.2.1. Private Keys can be transferred to adequate hardware security modules for back-up and recovery operations.

There's no stipulation for Keys belonging to other PKI participants.

6.2.7 Private key storage on cryptographic module

CA or RA private keys held on hardware cryptographic modules are stored in an encrypted form supported by the HSM vendor.

End-entity private keys must use encrypted containers compliant at least with FIPS 140-1 Level 1.

6.2.8 Method of activating private key

The private key in Certification Authorities in the **OGTM** is activated by initiating the PKI Software and activating the HSM where the key is stored. This process requires at least a dual-person control, except for Issuing CAs where automatic key activation in case of system failure or restart is allowed.

The activation of Subscriber's private key is stipulated in section 6.4.

6.2.9 Method of deactivating private key

The private key in Certification Authorities is deactivated by shutting-down the associated server or by terminating the PKI software or by extracting or shutting-down the HSM that contains the key. This task can be done by a System Administrator and, when planned, has to be notified and authorized to/from the CA Responsible.

Deactivating RA or other end-user private keys based in hardware is performed by the extraction of the secure device (smartcard or other accepted crypto-tokens) from the workstation it is used.

Deactivating of other end-user subscriber private keys, while not based in hardware, is accomplished by shutting down the device where the private key is stored. The subscriber must take all reasonable measures to avoid unauthorized use of the device.

6.2.10 Method of destroying private key

The procedure to destroy a private key is initiated in the following cases:

- Private Key is no longer used and it's mandated its destruction
- The token or HSM containing the key has deteriorated to an extent that prevents normal usage
- A lost or stolen token is found, and the keys it contained are suspected to be compromised

A private key can be destroyed by the key owner or a legal representative. In such cases the corresponding certificate will be revoked, and the community will be notified. The procedure used to destroy the private key depends on the particular container holding it, being responsibility of the individual executing the destruction doing it in an appropriate way. In particular, for private keys associated to CAs, this task must be executed under dual control and appropriate tracking information must be recorded.

6.2.11 Cryptographic Module Rating

No stipulation additional to section 6.2.1.

6.3 Other Aspects of Key Pair Management

This section includes additional stipulations regarding key pair management.

6.3.1 Public key archival

Public keys in the **OGTM** trust model are archived for a period of 7 years after the expiry or revocation of the corresponding digital certificate.

6.3.2 Certificate operational periods and key pair usage periods

The fully operational period for a certificate starts at the issuance and ends with the expiration or revocation of the certificate.

The validity period for key pairs is stipulated in the following table:

Certificate Type	Validity Period
OWGTM Root CA GA (SHA-1)	32 years
OWGTM Root CA GB/GC (SHA-2)	25 years
Policy Certification Authority	Up to the entire life time of the Root CA upon issuance
Issuing Certification Authority	Up to the entire life time of the Root CA upon issuance
End-Entity Certificate	*As stipulated in the appropriate CP.*

It must be understood that the validity period of a certificate can be limited by the own validity of the issuing Certification Authority.

The certificates are operational for signature validation and decryption from the issuance to the end of the archival period stated in 6.3.1.

6.4 Activation Data

This section stipulates the management of the data necessary to activate the private keys.

6.4.1 Activation data generation and installation

Activation data for Certification Authorities are generated and stored in cryptographic tokens and/or smart cards and are only used by authorized persons. In addition, these tokens require a password or PIN in order to enable the activation process.

Activations requiring a multi-person control will be enforced by splitting the activation data in several tokens.

Stipulations related to subscriber certificates are defined in the CPS published by the Issuing CA.

6.4.2 Activation data protection

Only the authorized persons know the password or PIN to activate the private keys. In the case of end-entities, only the certificate subscriber is entitled to know this information.

In all cases, the owner of the activation data is required to safeguard the secrecy of this information.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

The details of this information are classified and therefore not made public. The documents describing Computer Security Controls are only available for the people involved in the **OGTM** and only disclosed to accredited external parties for auditing purposes.

Certification and Registration Authorities operating under the **OGTM** Trust Model are required to meet these Security Controls. The compliance is periodically enforced by an auditing procedure.

6.5.1 Specific computer security technical requirements

OGTM enforces the use of the appropriate procedures and technical measures and systems in order to effectively control security risks. These include, but not limited to:

- Strong password policies
- Constant improvement of administration and operating procedures
- Physical isolation of confidential systems
- Antivirus and anti-malware detection systems
- Periodic internal security reviews

In particular, it is ensured the compliance with Baseline and Extended Validation requirements from the CA/Browser Forum, where applicable.

6.5.2 Computer security rating

OGTM establishes the computer ratings to be meet by the Certifications and Registration Authorities operating under the Trust Model. Compliance with these ratings is ensured by periodic internal audits.

6.6 Life Cycle Security Controls

This information is classified and is therefore not disclosed in detail. The detailed documents are available for review by external auditors after the appropriate authorization process.

6.6.1 System development controls

Systems are developed using the WISeKey KeySteps Methodology, which ensures the security and quality by setting a series of policies and operational and technical procedures controlling the building of the PKI components during all the phases of the project.

Authenticity and integrity of critical software components must be checked before they are enabled in a production environment, by using code signing or other acceptable methods.

6.6.2 Security management controls

The **OGTM** recommends following the ISO27000 security management approach. In particular WISeKey, as main operator of the Trust Model follows an informal adoption of such security standards.

6.6.3 Life cycle security controls

Life cycle and change-related security controls are ensured by the WISeKey KeySteps Methodology.

6.7 Network Security Controls

The **OGTM** enforces the adoption of effective controls to minimize any risk related to Network Security. The detailed information about these controls is classified and only made available for external auditors after the appropriate authorization process.

In particular, the server used for the **OGTM** Root CA are off-line systems, physically disconnected from any computer network, and all communication of sensitive information is protected using encryption and digital signature techniques.

6.8 Time-stamping

The **OGTM** provides a Time-Stamping Policy (**CertifyID TSP**) that regulates the operation of TimeStamp Authorities according to RFC3161. This service is made available by WISeKey as main Operator and other authorized entities adhering to the TSP. More information regarding time-stamping services and regulations is published in http://www.oiste.org/repository.

For other data requiring time and data information, as Certificates and CRLs, it's not mandatory to be cryptographic-based.

7 Certificate and CRL Profiles

All certificates issued under the **OGTM** are compliant to:

- ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 5280").

This section of the CPS is provided for general stipulation and as a reference to the specific Certificate Policy for each certificate type, available at http://www.oiste.org/repository. It must be understood that particular stipulations and mapping with subscriber certificates are found in the CPS published by the Issuing CAs affiliated to the OISTE Trust Model.

7.1 Certificate Profile

This section refers to the certificate profiles of Certification Authorities operating in the OISTE Trust Model.

The particular information on the subscriber certificates is stipulated in the appropriate CP.

7.1.1 Version number(s)

All certificates in the **OGTM** conform to X.509 Version 3.

7.1.2 Certificate extensions

For subordinate CA Certificates, **OGTM** mandates that new CAs created after 1st January 2019 must include appropriate EKU extensions, as mandated by the CABF Baseline Requirements and the main Root Certificate programs.

For subscriber certificates, this information is stipulated in the appropriate CP.

7.1.3 Algorithm object identifiers

For the Root CA and subordinate CA certificates, the used algorithms are:

- sha-1WithRSAEncryption
- sha256WithRSAEncryption
- ecdsa-with-sha384

For subscriber certificates, as stipulated in the appropriate CP.

7.1.4 Name forms

For CA certificates, the Subject Name, by combining adequate values for commonName, Organizational Unit, Organization and Country; conforms an identifier that uniquely identifies the CA and distinguishes it from other CAs in the Trust Model.

For subscriber certificates, as stipulated in the appropriate CP.

7.1.5 Name constraints

OGTM mandates that Issuing Certification Authorities not operated by WISeKey, as designated main operator, able to issue certificates including the EKU *serverAuthentication* or *emailProtection*, will be constrained for the issuance of certificates under a set of predefined and agreed names (domain names, e-mail suffixes or other name components). For exceptional cases where these constraints aren't applied,

these CAs will be included in the external audit for compliance assurance against any applicable requirement (including Baseline and Extended Validation Requirements from the CA/Browser Forum).

7.1.6 Certificate policy object identifier

An object identifier (OID) is a unique number that identifies an object or policy. The OIDs are administered by the **OGTM** and listed in the Annex B, "OID Inventory".

7.1.7 Usage of Policy Constraints extension

Issuing Certification Authorities will be appropriately constrained to be compliant with CA/Browser Forum and other requirements. Issuing CAs will be constrained to disallow the issuance of their own subordinated CAs and by controlling the key usages allowed in the end-user certificates. The correctness of this information is ensured by the audit tasks executed during the Key Creation Ceremony of the CA.

7.1.8 Policy qualifiers syntax and semantics

For subordinate CAs and for subscriber certificates, it's supported the inclusion of brief statements in Certificates about the limitations of liability and other terms associated with the use of a Certificate in the Policy Qualifier field of the Certificates Policy extension.

7.1.9 Processing semantics for the critical Certificate Policies extension

The "Certificate Policy" extension identifies the Policy that the **OGTM** assigned explicitly to a certificate profile. Software Applications requiring a specific certificate profile to process a digital signature must check this extension in order to verify the suitability of the certificate for the intended purpose.

7.2 CRL Profile

In general, CRLs generated under the **OGTM** Trust Model are compliant with RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002).

7.2.1 Version number(s)

CRLs conforming to X.509 Version 2 are supported in the **OGTM**.

7.2.2 CRL Profile and CRL entry extensions

CRL must include the following minimum extensions, as defined by the above standard:

- CRL Number
- Authority Key Identifier
- Revocation date
- Reason code

7.3 OCSP Profile

In general, the status of all certificates in the **OGTM**, except if indicated in the appropriate Certificate Policy, must be validated by sending requests compliant with RFC 6960.

OGTM ensures compliance with any applicable requirement from the CA/Browser Forum in terms of OCSP implementation for server authentication certificates.

7.3.1 Version number(s)

OGTM provides support for Version 1 of RFC6960.

7.3.2 OCSP extensions

No stipulation.

8 Compliance Audit and Other Assessment

OGTM monitors and ensures compliance to legal, security and industry requirements, in all levels of the Trust Model, through internal and external audits.

Those external and internal compliance audits are executed as defined by the CA/Browser Forum in its Baseline and Extended Validation Requirements. If applicable, other Industry and/or National assessment requirements can be fulfilled.

8.1 Frequency or circumstances of assessment

All Certification Authorities and dependent Registration Authorities must follow the adequate assessment program (as stipulated in section 8.4) on an annual frequency.

In particular for SSL certificates, the **OGTM** mandates the Issuing CAs to perform the required quarterly self-assessment, according to the CAB/Forum guidelines.

8.2 Identity/qualifications of assessor

The assessor will be selected when an audit or assessment is required. Any company or professional whose services are contracted as auditor or assessor will be required to fulfil these requirements:

- Adequate and accredited capability and experience to perform the required services (PKI audit, Security assessment, etc.). In particular for external audits, suitable accreditation to perform WebTrust audits is required.
- In the case of external audits, independent of the **OGTM** at an organization level.

8.3 Assessor's relationship to assessed entity

The **OGTM** audit policy does not allow any kind of legal, organizational or other relationship with the external auditor that would result in a conflict of interests.

8.4 Topics covered by assessment

The **OGTM** establishes two levels of audit and accreditation.

- The Root CA, Policy CAs and Issuing CAs owned or operated by WISeKey. These services are audited against the WebTrust criteria and commonly accepted industry accreditation standards. Issuing CAs operated by third parties which don't enforce name constraints must be included in this assessment.
- The Issuing CAs owned and/or operated by third parties enforcing name constraints and Registration Authorities. These services must meet the practices stipulated in this CPS, and the CPs that are entitled to issue, and are audited and accredited by the **OGTM** by means of an internal audit executed by WISeKey or other authorized auditor.

8.5 Actions taken as a result of deficiency

In the case a deficiency is identified, the **OGTM** will adopt and will be responsible for all necessary corrective measures.

In the case of a severe deficiency affecting the reliable operation of a Certification or a Registration Authority, the **OGTM** could decide to temporarily suspend the activities of the affected systems or services until the deficiency is solved.

8.6 Communication of results

All assessment results will be conformed as:

- Detailed Report. This document includes all the topics covered by the executed assessment program in detail. The detailed report is deemed private and only available to the following parties:
  - Certification Authority owner
  - **OGTM** Policy Approval Authority
- Audit Statement Report. This document only includes a formal statement from the auditor and reflects the result of the assessment, listing the topics covered and a global result. The summarized report is deemed public and is only published in the **OGTM** and Issuing Repository.

9 Other Business and Legal Matters

This section includes the stipulations for business and legal matters and should be understood as having a contractual value by all the PKI participants.

In this CPS are included stipulations affecting the Trust Model in general and the Root CAs in particular. The certificate subscribers and relying parties are required to check additional the appropriate CPS published by the Issuing CA. Certain sections could be stipulated in the appropriate CP document.

9.1 Fees

The fees applicable to the Certification Services covered by this CPS can be subject to variation according to specific agreement with the participants in the service. The detailed information of the fees is made available for the subscribers or other affected parties before enabling such services.

9.1.1 Certificate issuance or renewal fees

The issuance of certificates in the **OGTM** is considered a commercial service and therefore subject to fees. The fees depend on the certificate and project and are agreed before making it available to subscribers.

9.1.2 Certificate access fees

OGTM doesn't enforce stipulations for certificate access fees. In general, any participant shouldn't apply fees on the access to certificate information made public in the different repositories.

9.1.3 Revocation or status information access fees

OGTM doesn't enforce stipulations for revocation or status information access fees. In general, the Issuing CA shouldn't apply fees on the access to certificate information made public in the different repositories.

9.1.4 Fees for other services

The operators of Issuing CAs in the **OGTM** can set fees for different commercial services provided to parties willing to participate in the Trust Model. This includes, but not limited to:

- Managed PKI Services
- CA Signing Services
- CA Hosting and operation services

9.1.5 Refund policy

The refund policy applicable to commercial services provided by WISeKey is included in the "Subscriber agreement" and/or general Terms and Conditions communicated to the end-user when providing the service. Other refund policies can be established and, in such cases, must be effectively communicated to all affected parties.

9.2 Financial Responsibility

The **OGTM** established the adequate controls to ensure that the different levels of financial responsibility are met by the different participants, according to their impact in the trust model.

9.2.1 Insurance coverage

For the Root CA, Issuing CAs and the certification services provided directly by WISeKey, it is maintained an Errors and Omissions insurance policy that covers the liability expressed in section 9.8.

For affiliates and corporate customers acting as Certification or Registration Authorities, the contractual terms agreed among the parties ensure the assumed responsibilities for each party and transfer the requirement for appropriate insurance for the transferred liabilities.

9.2.2 Other assets

No stipulations.

9.2.3 Insurance or warranty coverage for end-entities

The maximum liability per subscriber certificate issued under the **OGTM** shall be established in the applicable CPS published by the Issuing CA.

9.3 Confidentiality of Business Information

In general, an Issuing CA under the **OGTM** may not disclose the confidential information of a subscriber, or use that information for any purpose, except:

- To its staff requiring the information for the purposes of this CPS or for delivery of the services.
- With the explicit consent of the subscriber.
- If required to do so by any law, or an applicable agreement.

9.3.1 Scope of confidential information

Information released to subscriber(s) or relying parties by Issuing CA may be considered confidential.

All Issuing CA under the **OGTM** shall keep the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- All private keys
- Any activation data used to access private keys or gain access to the CA system
- Any business continuity, incident response, contingency, and disaster recovery plans
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information
- Any information held by the Issuing CA in accordance with Section 9.4
- Any transactional, audit log and archive record identified in Section 5.4 or 5.5, including certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
- Transaction records, financial audit records and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS)
- All information classified explicitly as "PRIVATE", "CONFIDENTIAL" or "EXTRICTLY CONFIDENTIAL" when generated or exchanged among involved parties.

9.3.2 Information not within the scope of confidential information

The following information shall be deemed as non-confidential:

- All information contained in the issued certificates and Certificate Revocation Lists (CRLs) including all information that can be derived from such.
- All information classified expressly as "PUBLIC".

9.3.3 Responsibility to protect confidential information

The **OGTM Issuing CAs** are responsible of the protection of the confidential information generated or communicated during all operations. Delegated parties, as the entities managing subordinate Issuing CAs or Registration Authorities, are responsible for protecting confidential information that has been generated or stored by their own means.

For end entities, the certificate subscribers are responsible to protect their own private key and all activation information (i.e. passwords or PIN) needed to access or use the private key.

9.4 Privacy of Personal Information

The Issuing CAs operating in the **OGTM** must publish their own Privacy Policy and communicate it to the certificate subscribers in their CPS. This Policy must be compliant with the applicable requirements for international commercial services, and specifically with any applicable requirements from the CA/Browser Forum and European General Data Protection Regulation (GDPR).

In general, it must be understood that the CAs act as a "Data Controller" and the RAs and other parties involved in certificate management are "Data Processors" or, in certain occasions, "Joint Controllers".

9.4.1 Privacy plan

As stipulated in the CPS published by the subordinate CA.

9.4.2 Information treated as private

Personal information about an individual that is not publicly available in the contents of a certificate or CRL is considered private.

9.4.3 Information not deemed private

For personal information the provisions of section 9.3.2 apply respectively.

9.4.4 Responsibility to protect private information

The **OGTM** ensures the compliance of the legal obligations for Certification Authorities, Registration Authorities and other entities operating under the **OGTM** Trust Model. Each of these participants is responsible to protect the private information that has been provided by subscribers or other participants in the issuance and maintenance of digital certificates.

9.4.5 Notice and consent to use private information

In order to perform the certification provisioning service, the Issuing CAs and other parties interacting with certificate subscribers are required to obtain the consent to use the subscriber's personal information.

This consent is understood by the explicit acceptance of the "Terms and Conditions" and/or "End User Agreement" by the subscriber during the certificate request process. This acceptance is recognized by the subscriber's acceptance to obtain and install the certificate.

9.4.6 Disclosure pursuant to judicial or administrative process

The participants in the **OGTM** will disclose personal information of the participants if required by a judicial or administrative process, upon presentation of appropriate orders in accordance with the Applicable Laws of the country where the Certification Authority operates.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual Property Rights

All Intellectual Property rights, including the digital certificates and CRLs issued by the **OGTM Root CAs**, Object Identifiers, this CPS and the different CP are owned by the **OISTE Foundation**.

The private and public keys are the property of their respective owners.

Any commercial or protected trademark included in the Distinguished Name of a certificate is under responsibility of the certificate subscriber.

9.6 Representations and Warranties

This section includes general stipulations, specific terms can be stipulated in the appropriate Certificate Policy for a given certificate type and users community. If such is the case, specific Subscriber, Relying Party and other agreements will be distributed among the parties.

9.6.1 CA representations and warranties

OGTM Root CAs will:

- Establish a chain of trust by issuing a certificate, which is a self-signed certificate
- Ensure that the **Root** signs any subordinate CAs issued under the **OGTM** hierarchy
- Properly conduct the verification process described in section 3.2
- Ensure the accuracy and completeness of any part of the certificate information which is generated or compiled by the **OGTM**, according to the applicable Certification Policy
- Ensure that all relevant information concerning a certificate is recorded (electronically or otherwise) for an appropriate period of time, and in particular, for the purpose of providing evidence for the purposes of legal proceedings
- Utilize trustworthy systems, procedures and human resources in performing its services
- Comply with any other relevant provisions of the relevant CP or CPS, and other approved documents.

All CAs in the **OWGTM** will:

- Operate according to the requirements of this CPS and any applicable SLA.
- Ensure at the time it issues a certificate, that the certificate contains all the elements required by the CP or PDS.
- Manage their keys in accordance with *Section 6.2 Private Key Protection and Cryptographic Module Engineering Controls*.
- Ensure the availability of a Certificate Directory and CRL
- Promptly revoke a certificate if required.
- **MITM / traffic management policy**: Explicitly, the CAs will not issue a certificate that can be used for MITM or “traffic management” of domain names or IPs that the certificate holder does not

legitimately own or control. Therefore, the Issuing CA will be required to diligently execute the appropriate proofs of ownership or representation in the certificate issuance process.
- In particular and where applicable, CAs will respect the warranties and obligations set by the CA/Browser Forum Baseline and EV Requirements.

9.6.2 RA representations and warranties

The Registration Authorities operating under the **OGTM** warrant that:

- Will operate according to the requirements of this CPS.
- Their Certificates meet all material requirements of this CPS.
- No errors have been introduced in the Certificate information by the entities approving the Certificate Application as a result of a failure when managing the Certificate Application.
- There are no material misrepresentations of fact in the Certificate at the entities approving the Certificate Application or issuing the Certificate.
- Availability of revocation services (when applicable) and use of a repository conforming with the applicable CPS in all material aspects.

Registration Authority commercial contracts and agreements could include additional warranties.

9.6.3 Subscriber representations and warranties

The Subscribers of certificates issued under the **OGTM** must warrant that:

- All information supplied by the Subscriber and contained in the Certificate is true and valid.
- All representations made by the Subscriber in the submitted Certificate Application are true and valid.
- His or her private key is protected and that no unauthorized person has ever had access to the Subscriber's private key.
- An obligation and warranty that it will not install and use the Certificate(s) until it has reviewed and verified the accuracy of the data in each Certificate.
- An obligation and warranty to install the Certificate only on the server accessible at the domain name listed on the Certificate, and to use the Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement.
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS.
- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created.
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.
- An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request that the Certification Authority revokes the Certificate, in the event that: (a) any information in the Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key listed in the Certificate.
- An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an Certificate upon expiration or revocation of that Certificate.

The "Subscriber agreement" could include additional warranties.

9.6.4 Relying party representations and warranties

Before relying on a certificate or a digital signature, relying parties must:

- Validate the certificate and digital signature (including by checking whether or not it has been revoked, expired or suspended)
- Ascertain and comply with the purposes for which the certificate was issued and any other limitations on reliance or use of the certificate that are specified in this CPS.

If a relying party relies on a digital signature, or certificate, in circumstances where it has not been validated, it assumes all risks with regard to it (except those that would have arisen had the relying party validated the certificate), and is not entitled to any presumption that the digital signature is effective as the signature of the subscriber or that the certificate is valid.

Relying parties must also comply with any other relevant obligations specified in this CPS including those imposed on the entity when it is acting as a subscriber.

Additionally, the relying party should consider the certificate type. The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the relying party.

The "Relying party agreement" could include additional warranties.

9.6.5 Representations and warranties of other participants

No stipulations.

9.7 Disclaimers of Warranties

Other Disclaimer of warranties (if existing) is included as part of the agreement presented to each PKI participant, or included in the CPS published by the Issuing CA.

9.8 Limitations of Liability

Liability limitations are regulated in the contractual agreement between the concerned parties. If applicable such concepts are specified in the Subscriber, Relying Party or other commercial agreements made among the participants.

Subject to the foregoing limitations, **OGTM's** aggregate liability limit towards all End users, Relying Parties and any other entities that are not Subordinate PKI Entities for the whole of the validity period of certificates issued by the Root CA (unless revoked or suspended prior to its expiry) towards all persons with regard to such certificates is CHF 5,000,000.00 (Five Million Swiss Francs), with a maximum aggregate per year liability on such certificates of CHF 500,000.00 (Five Hundred and Thousand Swiss Francs). The OISTE Foundation delegates in WISeKey, as lead operator, this liability, according to a formal agreement executed between the parties, and that WISeKey ensures via an appropriate "Errors and Omissions" insurance.

9.9 Indemnities

Indemnities are regulated in the contractual agreement between the concerned parties. If applicable such concepts are specified in the CPS published but the Issuing CA, or in the Subscriber, Relying Party or other commercial agreements made among the participants.

9.10 Term and Termination

This section refers to the times and validity periods related to this document.

9.10.1 Term

This Document becomes effective once published in the **OGTM** Repository.

9.10.2 Termination

This Document (at the current version) is valid until replaced by a new version.

9.10.3 Effect of termination and survival

The Certificates issued during the validity period of the version of this document are bound to the clauses hereby included until the expiration of these certificates.

The termination of the CPS and its associated CP shall be without prejudice to the responsibility to protect confidential and personal information.

9.11 Individual notices and communications with participants

Notices to subscribers must be sent to the physical, postal, facsimile or email address of the subscriber, which is included in its registration information, or to another address that the subscriber has specified to the sender. Reasonable measures to ensure the reception of the notices are taken.

9.12 Amendments

The **OGTM** can unilaterally amend this document, by attaining adhering to the following procedure:

- The modification needs to be justified under legal and technical considerations.
- Any modification in the CPS cannot contradict the stipulations in the related CP, and vice-versa.
- There is a modification procedure and change management for these amendments.
- Any implications to the participants due to such amendments will be conveniently notified.

9.12.1 Procedure for amendment

The entity with the authority to make and approve any change in the CPS and the related CP in the **OGTM** is the **Policy Approval Authority** (PAA, described in section 1.5 of this document), which reviews the change request, assesses whether the change request is required, and approves the changes.

A change can only be made to the approved documents once approval has been granted by the PAA.

On the assumption that the PAA decides to modify the CPS or a particular CP, a new version of the document will be generated. The version of the document (exposed in all the pages of the document) is controlled with two numbers separated by a period. The first number (major version) is incremented if the new version could affect the acceptance of the certificates by the users. The second number (minor version) is incremented if the amendment is not considered to affect the certificate acceptance criteria. These two version numbers are included as the last two numbers in the OID identifying the document.

Once a new version of the document is approved, the procedures stipulated in section 9.12.2 will be executed.

9.12.2 Notification mechanism and period

Any modification in this document will be published in the **OGTM** website (http://www.oiste.org/repository) and affected participants will be directly notified if necessary.

In particular, it is not considered necessary to directly notify participants of "minor version" changes of the documents.

In the case of a change in the "major version" of a document, the **OGTM** may notify the affected participants with a digitally signed electronic message.

9.12.3 Circumstances under which OID must be changed

The OID of this CPS or a CP may be modified to reflect a change of major version of the document.

9.13 Dispute Resolution Procedures

As agreed between the parties by the acceptance of Subscriber and/or Relying Party agreements. If no prior agreement was made to the dispute resolution mechanism, general rules of law shall apply.

9.14 Governing Law

The CP, the CPS and the operations of the **OGTM** are all governed by the laws of Geneva, Switzerland.

9.15 Compliance with Applicable Law

All related parties shall comply with all applicable Swiss laws, rules, regulations, ordinances, and directives, and all provisions required thereby to be included in this CPS are hereby incorporated herein by reference.

Applicable national laws can affect parties operating Certification Authorities in different jurisdictions.

9.16 Miscellaneous Provisions

This section includes miscellaneous contractual and legal clauses.

9.16.1 Entire agreement

All provisions made in this CPs and the associated CP apply to all Certification and Registration Authorities operating under the **OGTM** and its subscribers.

Agreements or supplementary agreements by word of mouth are not allowed.

9.16.2 Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of WISeKey.

9.16.3 Severability

Should individual provisions of this CPS prove to be ineffective or incomplete, this shall be without prejudice to the effectiveness of all other provisions.

The ineffective provision will be replaced by an effective provision deemed as most closely reflecting the sense and purpose of the ineffective provision. In the case of incomplete provisions, amendment will be

agreed as deemed to correspond to what would have reasonably been agreed upon in line with the sense and purposes of this CPS, had the matter been considered beforehand.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

Force Majeure clauses, if existing, are included in the “Subscriber Agreement”.

9.17 Other Provisions

No stipulations.

10 Annex A: Glossary

AATL	Adobe Approved Trust List
CA	Certificate Authority or Certification Authority
CAA	Certification Authority Authorization
CAB	”CA/Browser” as in “CAB Forum”
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DBA	Doing Business As (also known as "Trading As")
DV	Domain Validated
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard FQDN Fully Qualified Domain Name
FTP	File Transfer Protocol
HISP	Health Information Service Provider
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers IdM Identity Management System
IDN	Internationalized Domain Name
ISSO	Information System Security Officer (also CSO, Chief Security Officer)
IETF	Internet Engineering Task Force
IGTF	International Grid Trust Federation
ITU	International Telecommunication Union
IV	Individual Validated
MICS	Member - Integrated Credential Service (IGTF) NIST National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validated
PAA	Policy Approval Authority
PIN	Personal Identification Number (e.g. a secret access code)
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments (at IETF.org)
SAN	Subject Alternative Name
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLD	Top - Level Domain
TLS	Transport Layer Security
TSA	Time Stamping Authority
TST	Time - Stamp Token
TTL	Time To Live
UTC	Coordinated Universal Time
X.509	The ITU - T standard for Certificates and their corresponding authentication framework

11 Annex B: OID Inventory

OWGTM enforces the use of the following OID Schema to identify the different Certificate Profiles issued under the whole PKI:

Public Arch:

2.16.756.5.14

<PUBLIC-ARCH>.4 – OISTE Certificate Policy Identifiers (legacy)

4.1 – Root CP

4.2 – Policy CA Class 1 CP (Standard)

4.2.1 – Issuing CA Class 1 CP

4.2.2 – Issuing CA Class 1 CP Extended

4.3 – Policy CA Class 2 CP- (Advanced)

4.3.1 – Issuing CA Class 2 CP

4.3.2.1 – Class 2 End Entity CPs

4.3.2.1.1 – CertifyID Advanced Individual Secure Mail

4.3.2.1.2 – CertifyID Advanced Individual Digital Signature

4.3.2.1.3 – CertifyID Advanced Corporate Digital Signature

4.3.2.1.4 – CertifyID Advanced SSL Certificate

4.4 – Policy CA Class 3 CP (Qualified)

4.4.1 – Issuing CA Class 3 CP

4.4.2.1 – Class 3 End Entity CPs

4.4.2.1.1 – CertifyID Qualified Individual

4.4.2.1.2 – CertifyID Qualified Corporate

4.4.2.1.3 – CertifyID Qualified Individual for Adobe

4.4.2.1.4 – CertifyID Qualified Corporate for Adobe

4.5 – Policy CA Class 4 CP

4.5.1 – Issuing CA Class 4 CP

4.6 – Pilot CP

4.7 – Time Stamping Service

4.7.1. – Time Stamp Policy CP

4.8 – OCSP Service

4.8.1. --- OCSP Policy CP

<PUBLIC-ARCH>.7 – OISTE Certificate Policy Identifiers (current)

7.1 – Root CP

7.2 – Policy CA CP

7.3 – Issuing CA CP

7.4 – End Entity CP

7.4.0 – CertifyID URA Admin Certificate

7.4.1 – CertifyID Personal Standard Certificate

7.4.2 – CertifyID Personal Advanced Certificate

7.4.3 – CertifyID Corporate Advanced Certificate

7.4.4 – CertifyID Personal Qualified Certificate

7.4.5 – CertifyID Corporate Qualified Certificate

7.4.6 – CertifyID Standard SSL Certificate

7.4.7 – CertifyID Advanced OV SSL Certificate

7.4.8 – CertifyID Advanced EV SSL Certificate

7.4.9 – CertifyID Code Signing Certificate

7.4.10 – CertifyID EV Code Signing Certificate

7.5 – Pilot CP

7.6 – Time Stamp Policy CP

7.7 – OCSP Service

<PUBLIC-ARCH>.8 – Policy qualifiers for special purposes

8.1 – Vendor specific OID

8.1.1 – Qualifier for Adobe PDF (AATL)

8.2 – Device certificates

8.2.1 – CertifyID Device Certificate