OISTE/WISeKey Global Trust Model CP/CPS

Version 4.1

OISTE Policy Approval Authority

November 26, 2025 (Release 4.1)

VERSION	DATE	MODIFICATION	AUTHOR
4.0	9/12/2024	First consolidated CP/CPS	Pedro Fuentes
4.0.1	13/1/2025	Minor changes	Pedro Fuentes
4.0.2	21/3/2025	Minor changes	Pedro Fuentes
4.0.3	27/6/2025	Minor changes	Pedro Fuentes
4.0.4	DRAFT	Statement for Mass Revocation	Pedro Fuentes
4.1	26/11/2025	Wording improvements to address root program feedback	Pedro Fuentes

Contents

1. INTRODUCTION **9**
1.1 Overview . . . 9
1.2 Document name and identification . . . 10
1.3 PKI participants . . . 10
1.3.1 Certification authorities . . . 10
1.3.2 Registration authorities . . . 10
1.3.3 Subscribers . . . 11
1.3.4 Relying parties . . . 11
1.3.5 Other participants . . . 11
1.4 Certificate usage . . . 11
1.4.1 Appropriate certificate uses . . . 11
1.4.2 Prohibited certificate uses . . . 15
1.5 Policy administration . . . 15
1.5.1 Organization administering the document . . . 15
1.5.2 Contact person . . . 15
1.5.3 Person determining CPS suitability for the policy . . . 15
1.5.4 CPS approval procedures . . . 15
1.6 Definitions and acronyms . . . 15

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES **15**
2.1 Repositories . . . 15
2.2 Publication of certification information . . . 16
2.2.1 Statement on Compliance with CA/Browser Forum requirements . . . 16
2.3 Time or frequency of publication . . . 16
2.4 Access controls on repositories . . . 16

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 or pseudonymity of subscribers . . . 17
3.1.4 Rules for interpreting various name forms . . . 17
3.1.5 Uniqueness of names . . . 17
3.1.6 Recognition, authentication, and role of trademarks . . . 17
3.2 Initial identity validation . . . 17
3.2.1 Method to prove possession of private key . . . 17
3.2.2 Authentication of organization identity . . . 17
3.2.2.6 Email Challenge Response Procedure . . . 20
3.2.3 Authentication of individual identity . . . 20
3.2.4 Non-verified subscriber information . . . 21
3.2.5 Validation of authority . . . 21
3.2.6 Criteria for interoperation . . . 22
3.3 Identification and authentication for re-key requests . . . 22
3.3.1 Identification and authentication for routine re-key . . . 22
3.3.2 Identification and authentication for re-key after revocation . . . 22
3.4 Identification and authentication for revocation request . . . 22

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS **22**
4.1 Certificate Application . . . 23
4.1.1 Who can submit a certificate application . . . 23
4.1.2 Enrollment process and responsibilities . . . 23
4.2 Certificate application processing . . . 23
4.2.1 Performing identification and authentication functions . . . 23
4.2.2 Approval or rejection of certificate applications . . . 25
4.2.3 Time to process certificate applications . . . 25

4.3 Certificate issuance . . . 25
4.3.1 CA actions during certificate issuance . . . 25
4.3.2 Notification to subscriber by the CA of issuance of certificate . . . 25
4.4 Certificate acceptance . . . 25
4.4.1 Conduct constituting certificate acceptance . . . 25
4.4.2 Publication of the certificate by the CA . . . 26
4.4.3 Notification of certificate issuance by the CA to other entities . . . 26
4.5 Key pair and certificate usage . . . 26
4.5.1 Subscriber private key and certificate usage . . . 26
4.5.2 Relying party public key and certificate usage . . . 26
4.6 Certificate renewal . . . 26
4.6.1 Circumstance for certificate renewal . . . 26
4.6.2 Who may request renewal . . . 26
4.6.3 Processing certificate renewal requests . . . 26
4.6.4 Notification of new certificate issuance to subscriber . . . 26
4.6.5 Conduct constituting acceptance of a renewal certificate . . . 26
4.6.6 Publication of the renewal certificate by the CA . . . 27
4.6.7 Notification of certificate issuance by the CA to other entities . . . 27
4.7 Certificate re-key . . . 27
4.7.1 Circumstance for certificate re-key . . . 27
4.7.2 Who may request certification of a new public key . . . 27
4.7.3 Processing certificate re-keying requests . . . 27
4.7.4 Notification of new certificate issuance to subscriber . . . 27
4.7.5 Conduct constituting acceptance of a re-keyed certificate . . . 27
4.7.6 Publication of the re-keyed certificate by the CA . . . 27
4.7.7 Notification of certificate issuance by the CA to other entities . . . 27
4.8 Certificate modification . . . 27
4.8.1 Circumstance for certificate modification . . . 27
4.8.2 Who may request certificate modification . . . 27
4.8.3 Processing certificate modification requests . . . 28
4.8.4 Notification of new certificate issuance to subscriber . . . 28
4.8.5 Conduct constituting acceptance of modified certificate . . . 28
4.8.6 Publication of the modified certificate by the CA . . . 28
4.8.7 Notification of certificate issuance by the CA to other entities . . . 28
4.9 Certificate revocation and suspension . . . 28
4.9.1 Circumstances for revocation . . . 28
4.9.2 Who can request revocation . . . 29
4.9.3 Procedure for revocation request . . . 29
4.9.4 Revocation request grace period . . . 30
4.9.5 Time within which CA must process the revocation request . . . 30
4.9.6 Revocation checking requirement for relying parties . . . 30
4.9.7 CRL issuance frequency . . . 30
4.9.8 Maximum latency for CRLs . . . 30
4.9.9 On-line revocation/status checking availability . . . 30
4.9.10 On-line revocation checking requirements . . . 31
4.9.11 Other forms of revocation advertisements available . . . 31
4.9.12 Special requirements re key compromise . . . 31
4.9.13 Circumstances for suspension . . . 31
4.9.14 Who can request suspension . . . 31
4.9.15 Procedure for suspension request . . . 31
4.9.16 Limits on suspension period . . . 31
4.10 Certificate status services . . . 31
4.10.1 Operational characteristics . . . 31
4.10.2 Service availability . . . 31
4.10.3 Optional features . . . 32
4.11 End of subscription . . . 32

4.12 Key escrow and recovery . . . 32
4.12.1 Key escrow and recovery policy and practices . . . 32
4.12.2 Session key encapsulation and recovery policy and practices . . . 32

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 32
5.1 Physical controls . . . 33
5.1.1 Site location and construction . . . 33
5.1.2 Physical access . . . 33
5.1.3 Power and air conditioning . . . 33
5.1.4 Water exposures . . . 33
5.1.5 Fire prevention and protection . . . 33
5.1.6 Media storage . . . 33
5.1.7 Waste disposal . . . 33
5.1.8 Off-site backup . . . 33
5.2 Procedural controls . . . 34
5.2.1 Trusted roles . . . 34
5.2.2 Number of persons required per task . . . 34
5.2.3 Identification and authentication for each role . . . 34
5.2.4 Roles requiring separation of duties . . . 34
5.3 Personnel controls . . . 34
5.3.1 Qualifications, experience, and clearance requirements . . . 34
5.3.2 Background check procedures . . . 35
5.3.3 Training requirements . . . 35
5.3.4 Retraining frequency and requirements . . . 35
5.3.5 Job rotation frequency and sequence . . . 35
5.3.6 Sanctions for unauthorized actions . . . 35
5.3.7 Independent contractor requirements . . . 35
5.3.8 Documentation supplied to personnel . . . 36
5.4 Audit logging procedures . . . 36
5.4.1 Types of events recorded . . . 36
5.4.2 Frequency of processing log . . . 37
5.4.3 Retention period for audit log . . . 37
5.4.4 Protection of audit log . . . 37
5.4.5 Audit log backup procedures . . . 37
5.4.6 Audit collection system (internal vs. external) . . . 37
5.4.7 Notification to event-causing subject . . . 37
5.4.8 Vulnerability assessments . . . 37
5.5 Records archival . . . 38
5.5.1 Types of records archived . . . 38
5.5.2 Retention period for archive . . . 38
5.5.3 Protection of archive . . . 38
5.5.4 Archive backup procedures . . . 38
5.5.5 Requirements for time-stamping of records . . . 38
5.5.6 Archive collection system (internal or external) . . . 38
5.5.7 Procedures to obtain and verify archive information . . . 38
5.6 Key changeover . . . 38
5.7 Compromise and disaster recovery . . . 39
5.7.1 Incident and compromise handling procedures . . . 39
5.7.2 Computing resources, software, and/or data are corrupted . . . 40
5.7.3 Entity private key compromise procedures . . . 40
5.7.4 Business continuity capabilities after a disaster . . . 40
5.8 CA or RA termination . . . 40

6. TECHNICAL SECURITY CONTROLS 41
6.1 Key pair generation and installation . . . 41
6.1.1 Key pair generation . . . 41
6.1.2 Private key delivery to subscriber . . . 42

6.1.3 Public key delivery to certificate issuer . . . 42
6.1.4 CA public key delivery to relying parties . . . 42
6.1.5 Key sizes . . . 42
6.1.6 Public key parameters generation and quality checking . . . 42
6.1.7 Key usage purposes (as per X.509 v3 key usage field) . . . 42
6.2 Private Key Protection and Cryptographic Module Engineering Controls . . . 43
6.2.1 Cryptographic module standards and controls . . . 43
6.2.2 Private key (n out of m) multi-person control . . . 43
6.2.3 Private key escrow . . . 43
6.2.4 Private key backup . . . 43
6.2.5 Private key archival . . . 43
6.2.6 Private key transfer into or from a cryptographic module . . . 43
6.2.7 Private key storage on cryptographic module . . . 43
6.2.8 Method of activating private key . . . 43
6.2.9 Method of deactivating private key . . . 44
6.2.10 Method of destroying private key . . . 44
6.2.11 Cryptographic Module Rating . . . 44
6.3 Other aspects of key pair management . . . 44
6.3.1 Public key archival . . . 44
6.3.2 Certificate operational periods and key pair usage periods . . . 44
6.4 Activation data . . . 45
6.4.1 Activation data generation and installation . . . 45
6.4.2 Activation data protection . . . 45
6.4.3 Other aspects of activation data . . . 45
6.5 Computer security controls . . . 45
6.5.1 Specific computer security technical requirements . . . 45
6.5.2 Computer security rating . . . 46
6.6 Life cycle technical controls . . . 46
6.6.1 System development controls . . . 46
6.6.2 Security management controls . . . 46
6.6.3 Life cycle security controls . . . 46
6.7 Network security controls . . . 46
6.8 Time-stamping . . . 47

7. CERTIFICATE, CRL, AND OCSP PROFILES 47
7.1 Certificate profile . . . 47
7.1.1 Version number(s) . . . 47
7.1.2 Certificate extensions . . . 47
7.1.3 Algorithm object identifiers . . . 48
7.1.4 Name forms . . . 48
7.1.5 Name constraints . . . 48
7.1.6 Certificate policy object identifier . . . 48
7.1.7 Usage of Policy Constraints extension . . . 48
7.1.8 Policy qualifiers syntax and semantics . . . 48
7.1.9 Processing semantics for the critical Certificate Policies extension . . . 48
7.2 CRL profile . . . 48
7.2.1 Version number(s) . . . 48
7.2.2 CRL and CRL entry extensions . . . 49
7.3 OCSP profile . . . 50
7.3.1 Version number(s) . . . 50
7.3.2 OCSP extensions . . . 50

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 50
8.1 Frequency or circumstances of assessment . . . 51
8.2 Identity/qualifications of assessor . . . 51
8.3 Assessor's relationship to assessed entity . . . 51
8.4 Topics covered by assessment . . . 51

8.5 Actions taken as a result of deficiency . . . 51
8.6 Communication of results . . . 51
8.7 Self-Audits . . . 51

9. OTHER BUSINESS AND LEGAL MATTERS 52
9.1 Fees . . . 52
9.1.1 Certificate issuance or renewal fees . . . 52
9.1.2 Certificate access fees . . . 52
9.1.3 Revocation or status information access fees . . . 52
9.1.4 Fees for other services . . . 52
9.1.5 Refund policy . . . 52
9.2 Financial responsibility . . . 52
9.2.1 Insurance coverage . . . 52
9.2.2 Other assets . . . 52
9.2.3 Insurance or warranty coverage for end-entities . . . 52
9.3 Confidentiality of business information . . . 53
9.3.1 Scope of confidential information . . . 53
9.3.2 Information not within the scope of confidential information . . . 53
9.3.3 Responsibility to protect confidential information . . . 53
9.4 Privacy of personal information . . . 53
9.4.1 Privacy plan . . . 53
9.4.2 Information treated as private . . . 53
9.4.3 Information not deemed private . . . 54
9.4.4 Responsibility to protect private information . . . 54
9.4.5 Notice and consent to use private information . . . 54
9.4.6 Disclosure pursuant to judicial or administrative process . . . 54
9.4.7 Other information disclosure circumstances . . . 54
9.5 Intellectual property rights . . . 54
9.6 Representations and warranties . . . 54
9.6.1 CA representations and warranties . . . 54
9.6.2 RA representations and warranties . . . 55
9.6.3 Subscriber representations and warranties . . . 55
9.6.4 Relying party representations and warranties . . . 55
9.6.5 Representations and warranties of other participants . . . 56
9.7 Disclaimers of warranties . . . 56
9.8 Limitations of liability . . . 56
9.9 Indemnities . . . 56
9.10 Term and termination . . . 56
9.10.1 Term . . . 56
9.10.2 Termination . . . 56
9.10.3 Effect of termination and survival . . . 56
9.11 Individual notices and communications with participants . . . 57
9.12 Amendments . . . 57
9.12.1 Procedure for amendment . . . 57
9.12.2 Notification mechanism and period . . . 57
9.12.3 Circumstances under which OID must be changed . . . 57
9.13 Dispute resolution provisions . . . 57
9.14 Governing law . . . 57
9.15 Compliance with applicable law . . . 57
9.16 Miscellaneous provisions . . . 58
9.16.1 Entire agreement . . . 58
9.16.2 Assignment . . . 58
9.16.3 Severability . . . 58
9.16.4 Enforcement (attorneys' fees and waiver of rights) . . . 58
9.16.5 Force Majeure . . . 58
9.17 Other provisions . . . 58

Appendix A: Glossary **58**
Acronyms . . . 58
Definitions . . . 59

Appendix B: CA Hierarchies **62**
Legacy OISTE Root "Generation A" . . . 62
Root Information . . . 62
Subordinate CA Information . . . 62
Legacy OISTE Root "Generation B" . . . 62
Root Information . . . 62
Subordinate CA Information . . . 62
Legacy OISTE Root "Generation C" . . . 63
Root Information . . . 63
Subordinate CA Information . . . 63
New OISTE Root for Client/Personal certificates (ECC) "Generation 1" . . . 63
Root Information . . . 63
Subordinate CA Information . . . 63
New OISTE Root for Client/Personal certificates (RSA) "Generation 1" . . . 63
Root Information . . . 63
Subordinate CA Information . . . 63
New OISTE Root for TLS Server certificates (ECC) "Generation 1" . . . 64
Root Information . . . 64
Subordinate CA Information . . . 64
New OISTE Root for TLS Server certificates (RSA) "Generation 1" . . . 64
Root Information . . . 64
Subordinate CA Information . . . 64

Appendix C: OID Inventory **64**

Appendix D: Certificate Profiles **65**
Infrastructure Certificates . . . 65
Issuing CA Certificates . . . 65
OCSP Responder Certificates . . . 66
TLS Certificate Profiles . . . 67
TLS Certificates Validity Period Schedule . . . 67
DV TLS Certificate Profile . . . 67
OV TLS Certificate Profile . . . 68
EV TLS Certificate Profile . . . 69
S/MIME Certificate Profiles . . . 69
S/MIME Certificates Validity Period Schedule . . . 70
Mailbox-Validated Certificate Profile . . . 70
Individual-Validated Certificate Profile . . . 71
Sponsor-Validated Certificate Profile . . . 72
Organization-Validated Certificate Profile . . . 73
Non-S/MIME Personal/Device Certificate Profiles . . . 74

Appendix E: Version history **74**
Combined CP/CPS document (this document) . . . 74
Previous versions . . . 74

1. INTRODUCTION

This document represents a combined Certificate Policy (CP) and Certification Practice Statement (CPS), and describes the practices followed with regard to the management of the lifecycle the Certification Authorities adhered to the OISTE/WISeKey Global Trust Model (OWGTM from now on).

1.1 Overview

The main two legal entities involved in the control and operation of the OISTE/WISeKey Global 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 (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 this document.

The OISTE/WISeKey Global Trust Model (OWGTM) 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 OWGTM 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 OWGTM for the issuance of digital certificates. It is organized in the following sections: 1. Introductions – This section. Introduces the OWGTM 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. 1. Identification and Authentication – Discloses the rules for subscriber naming and required authentication policies. 1. Certificate Life-Cycle Operational Requirements – This section describes the different phases in the Life-Cycle of certificates and their requirements. 1. Management, Operational and Physical Controls – Describes the controls enforced in the OWGTM to provide adequate trust levels in the certificates issued under the Trust Model. 2. Technical Security Controls – Discloses the security controls adopted in the OWGTM. 3. Certificate and CRL Profiles – Describes the technical details of the different certificate types issued under the OWGTM. 1. Compliance Audit and other Assessment – Discloses the audit policies followed in the OWGTM to ensure that the participant fulfils the security and quality requirements. 1. Other Business and Legal Matters – This section exposes the commercial, legal and contractual aspects involved in the usage of certificates issued in the OWGTM.

APPLICABILITY NOTICE: If any inconsistency exists between this document and the normative provisions of an applicable industry guideline or standard ("Applicable Requirements"), then the Applicable Requirements take precedence over this CP/CPS.

1.2 Document name and identification

Name	OISTE/WISeKey Global Trust Model Certificate Policy/Certification Practices Statement (CP/CPS)
Version	4.1
OID	2.16.756.5.14.7.1
Issuance date	26/11/2025
Location	This document is linked in https://oiste.org/repository and https://wisekey.com/repository

1.3 PKI participants

The following sections describe the different participant types in the OWGTM.

1.3.1 Certification authorities

OISTE and WISeKey own and operate a number of Root and Issuing Certification Authorities (CAs) hierarchies that deliver certification Services under this CP/CPS.

These hierarchies are detailed in Appendix B of this document.

OISTE and WISeKey also own and operate a number of Time Stamping Authorities (TSA), which are regulated by their corresponding Time Stamping Policy (TSP) document.

1.3.2 Registration authorities

The Registration Authorities (RA) are the physical or legal persons responsible for the identification of the entities requesting a certificate (referred as “applicants” when the request is in process and “subscribers” for those in possession of a certificate). The OWGTM delegates to Registration Authorities the responsibility of verifying the information provided by the applicant within a certificate request, ensuring that the request and the process used to deliver the certificate to the subscriber meets the requirements of this CPS and the appropriate CP.

The Registration Authorities in the OWGTM are directly supervised by the CA and follow an accreditation process imposed by the CA in order to ensure that all security and operational procedures related to the certificates life-cycle are strictly enforced. Within the OWGTM environment there exist locations named “OWGTM Registration Point” that are the physical or virtual locations where a Registration Authority operates. These Registration Points are operated by “Registration Authority Officers”, who are authorized persons responsible for verifying the identity and veracity of a certificate request for an end entity and the delivery of the certificate once issued by the Certification Authority.

Therefore, the responsibilities of Registration Authorities operating under the OWGTM are as follows: - Check the identity and circumstances needed to verify that a certificate request is valid according to the type of certificate requested. - Inform the applicant, before the issuance of the certificate, about the terms and conditions related to the certificate and its usage. - Verify that the information contained in a certificate is exact and complete according to the requirements of the corresponding CP. - Ensure that the subscriber is in possession of the digital signature creation data (private keys) associated to the certificate to be issued.

OWGTM may delegate identity vetting and application intake to accredited RAs under written contracts requiring adherence to this CPS, audit rights and security controls. OWGTM will maintain oversight and perform periodic audits of each RA.

Currently is not supported the existence of Registration Authorities which are entitled to issue TLS, S/MIME or Code Signing certificates without the participation of WISeKey for the domain or mailbox validation. WISeKey supports the concept of “Managed PKI” services for pre-authorized organizations and their validated internet domains.

1.3.3 Subscribers

In the OWGTM two different end-user roles are defined. Depending on the status of the certificate request, these roles are named "Applicant" and "Subscriber". - An applicant is a physical person that requests a certificate for his own behalf or on behalf of a third party. The applicant needs to accredit his identity and ability to request a certificate. In the case of an applicant acting on behalf of a third party or legal person, he will be requested to accredit the empowerment for such representation, as required by law. - A subscriber is the physical or legal person whose identity is linked to the electronic signature creation data, or private key, and included in a digital certificate. In general, a subscriber is considered the "owner" of a certificate. The subscriber of a certificate is responsible for the custody of his private key and not communicating this data in any way to any other person.

This document details the particular community of subscribers to whom each type of certificate is aimed and what identification and other security requirements should be fulfilled.

1.3.4 Relying parties

All natural and legal persons and other entities that trust the certificates issued by certification authorities operating under the OWGTM Trust Model are considered to be "relying parties". These relying parties do not necessarily need to be a subscriber of an OWGTM certificate, but are requested to accept the "CertifyID Relying Party agreement", available at http://oiste.org/repository.

In the OWGTM, a particular type of certificate could limit the right to be a relying party for that particular type of certificate, if this is the case, a specific Relying Party agreement would be published.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

In the OWGTM, the limitations for certificate usage are established for each particular certificate type. This information is summarized in the following subsections. The type of certificate is determined by the combination of "Key Usage", "Extended Key Usage", and Policy Identifiers.

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 model	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

Certificate type	Description	Permitted uses
Standard (Basic) Personal Certificate	Low Assurance Personal certificates used by Natural persons to authenticate and encrypt documents and transactions. Only the eMail address is verified and included in the certificate.**When used for email Protection, this is equivalent to the "mailbox-validated" profile defined by the CAB/Forum Baseline Requirements for S/MIME Certificates**	Digital Signature, Encryption, Client Authentication and email Protection
Advanced Personal Certificate	High Assurance Personal certificates with software keys, used by Natural person to authenticate and encrypt documents and transactions. Personal identity attributes are validated and included in the certificate. Remote verification is allowed under certain circumstances.**When used for email Protection, this is equivalent to the "individual-validated" profile defined by the CAB/Forum Baseline Requirements for S/MIME Certificates**	Digital Signature, Encryption, Client Authentication and email Protection
Qualified Personal Certificate	High Assurance Personal certificates with software or hardware keys, used by Natural person to authenticate and encrypt documents and transactions. Valid for Advanced Signatures of PDF documents. Personal identity attributes are validated and included in the certificate. Remote verification is allowed under certain circumstances.**When used for email Protection, this is equivalent to the "individual-validated" profile defined by the CAB/Forum Baseline Requirements for S/MIME Certificates**	Digital Signature, Encryption, Non-Repudiation, Client Authentication, Document Signing and email Protection

Certificate type	Description	Permitted uses
Advanced Professional Certificate	High Assurance Personal certificates with software keys, used by Natural person to authenticate and encrypt documents and transactions. Personal identity and Organization attributes are validated and included in the certificate. Remote verification is allowed under certain circumstances.**When used for email Protection, this is equivalent to the "sponsor-validated" profile defined by the CAB/Forum Baseline Requirements for S/MIME Certificates**	Digital Signature, Encryption, Client Authentication and email Protection
Qualified Professional Certificate	High Assurance Personal certificates with software or hardware keys, used by Natural person to authenticate and encrypt documents and transactions. Valid for Advanced Signatures of PDF documents. Personal identity and Organization attributes are validated and included in the certificate. Remote verification is allowed under certain circumstances.**When used for email Protection, this is equivalent to the "sponsor-validated" profile defined by the CAB/Forum Baseline Requirements for S/MIME Certificates**	Digital Signature, Encryption, Non-Repudiation, Client Authentication, Document Signing and email Protection
Advanced Corporate Certificate	High Assurance Corporate certificates with software keys, used by Legal person to authenticate and encrypt documents and transactions. Organization attributes are validated and included in the certificate. Remote verification is allowed under certain circumstances.**When used for email Protection, this is equivalent to the "organization-validated" profile defined by the CAB/Forum Baseline Requirements for S/MIME Certificates**	Digital Signature, Encryption, Client Authentication and email Protection

Certificate type	Description	Permitted uses
Qualified Corporate Certificate	High Assurance Corporate certificates with software or hardware keys, used by Legal person to authenticate and encrypt documents and transactions. Valid for Advanced Signatures of PDF documents. Organization attributes are validated and included in the certificate. Remote verification is allowed under certain circumstances.**When used for email Protection, this is equivalent to the "organization-validated" profile defined by the CAB/Forum Baseline Requirements for S/MIME Certificates**	Digital Signature, Encryption, Non-Repudiation, Client Authentication, Document Signing and email Protection
DV TLS Certificate	Medium assurance TLS certificate. All identification attributes in the certificate are verified. The control on the Internet Domain is validated. Compliant with CA/Browser Forum Baseline Requirements	Digital Signature, Encryption, Server Authentication
OV TLS Certificate	High assurance TLS certificate. All identification attributes in the certificate are verified. The Identity of the organization is validated. Compliant with CA/Browser Forum Baseline Requirements	Digital Signature, Encryption, Server Authentication
EV TLS Certificate	High assurance TLS certificate compliant. All identification attributes in the certificate are verified. The Identity of the organization is validated. Compliant with CA/Browser Requirements for Extended Validation	Digital Signature, Encryption, Server Authentication
Device Certificate	High Assurance Device certificates used by devices to authenticate themselves and to protect transactions over IoT networks. Identity information as model number, serial number and manufacturer information are validated. Remote validation is allowed under certain circumstances	Digital Signature, Encryption, Client Authentication

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

This section describes how this document is administered. The same practices apply to all policies adopted by the OWGTM.

1.5.1 Organization administering the document

This document is administered by the OWGTM 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 and WISeKey. 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 and WISeKey.

1.5.2 Contact person

- **Name:** OISTE Foundation - OWGTM Policy Approval Authority
- **email address:** cps@oiste.org, cps@wisekey.com
- **Address:** Avenue Louis-Casaï 58 - 1216 Cointrin - Switzerland

This same contact can also be used for revocation requests and compliance-related notifications.

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 OWGTM PAA.

1.5.4 CPS approval procedures

The OWGTM 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 OWGTM 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 CP/CPS, 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.

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

The version history for this combined CP/CPS document is included in Appendix E. Version history.

1.6 Definitions and acronyms

Definitions and Acronyms are included in Appendix A

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The main repositories of the OWGTM are: - Policies repository for disclosure of CP/CPS and related information. This repository is a set of web pages and services available at the URLs https://oiste.org and

https://wisekey.com/repository - Certificate and Certificate Revocation information repositories. The CA certificates and Certificate Revocation Information sources are included, when relevant, as CDP and AIA extensions in the certificates issued under the OISTE Root CAs - Public Certificate repositories, as described in the following section.

2.2 Publication of certification information

The OWGTM is responsible for publication of information regarding practices, certificates, and the current status of certificates. Publicly accessible certificate information repositories is maintained through the certificate management platforms operating under the OWGTM are disclosed appropriately to the relying parties of these certificates.

The shared repositories containing public information in the OWGTM are managed by 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 and WISeKey ensure the compliance with industry best practices and security controls. In particular, the trust model enforces regular review and compliance with the latest version of the "Baseline Requirements" and "Extended Validation Requirements" for the certificate profiles to which these regulations apply (these requirements are available respectively at https://cabforum.org/)

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 this CPS.

2.3 Time or frequency of publication

The CP/CPS 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 OWGTM 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 controls on repositories

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

3. IDENTIFICATION AND AUTHENTICATION

The OWGTM mandates the fulfillment 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

3.1 Naming

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

3.1.1 Types of names

All subscribers are assigned a Distinguished Name (DN) conforming to ITU X.500. This DN is composed of a Common Name (CN), which includes a unique identification of the subscriber, 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 or pseudonymity of subscribers

In general, the use of anonymity or pseudonymity is always controlled by the applicable regulations: - Allowed, but discouraged for Personal Certificates - Disallowed for TLS Server certificates

3.1.4 Rules for interpreting various name forms

The rules used in the OWGTM to interpret the distinguished names of certificates issued under its Trust Model are defined by the RFC 2253 and ITU-T X.520 standards.

3.1.5 Uniqueness of names

OWGTM requires uniqueness of names in the certificates issued by the Roots, except in the case of re-issuances or renewals for the same entity.

For subscriber certificates, uniqueness of certificates is generally not enforced.

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 OWGTM nor the applicant, nor the subscriber. The OWGTM 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.

OWGTM – Root CA Certification Practices Statement (CPS) In any event, the OWGTM will not attempt to intermediate nor resolve conflicts regarding ownership of names or trademarks.

3.2 Initial identity validation

OWGTM performs “face to face” identity validation for the certificates issued by the Roots. Stipulations related to subscriber certificates are defined in the following sections.

In general, any Issuing CA operating in the OWGTM and issuing TLS/TLS or S/MIME certificates, must ensure compliance with the baseline requirements and extended validation guidelines mandated by the CA/Browser Forum, as detailed in this section.

Sources used for S/MIME and EV validation can be found at https://wisekey.com/repository.

OWGTM performs an evaluation and approval Prior to relying upon a third-party data source as a “Reliable Data Source” for identity or DBA/organization validation. This evaluation includes: (a) provenance and authority (is it a recognized government or registered business registry?), (b) accuracy (currency and update frequency), (c) resistance to alteration or falsification (controls on write access, presence of cryptographic protections if applicable), (d) availability, and (e) whether the validation process can independently corroborate results from the source. The evaluation outcome and authorization to use the source is be recorded and versioned. Re-evaluation and review of the sources list is performed whenever needed.

3.2.1 Method to prove possession of private key

If the key pair is generated by the End Entity (applicant or future subscriber), then a demonstration of the possession of the private key associated to the public key is requested. Accepted means are the generation of a Certificate Signing Request (CSR) linked to the private key, or any other method accepted by OWGTM.

If (when allowed by the applicable regulations) the key pair is generated by the CA or the RA, OWGTM defines and enforces approved procedures to transfer securely the private key to the subscriber (i.e. sending PFX files and passwords by different channels, and deleting any signature private key once the transfer is effective).

3.2.2 Authentication of organization identity

Before issuing a certificate for a subordinate Certification Authority OWGTM 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.

3.2.2.1 Organization Identity validation If the Certificate's SubjectDN is to include the name or address of an organization, the RA shall verify the identity and address of the organization and that the address is the Applicant's address of existence or operation.

OWGTM's appointed RA shall verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following: - A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition; - A third-party database that is periodically updated and considered a Reliable Data Source as defined in the introduction of this section 3.2; - A site visit by OWGTM or a third party who is acting as an agent for OWGTM; or - An Attestation Letter.

Acceptable documentation may include: - Articles of incorporation
- Government-issued business registration certificate
- Recent financial / statutory document (if required by policy)

The RA should perform **out-of-band verification**, where necessary, such as phone verification or email verification to a known domain address.

OWGTM may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other reliable form of identification.

For the issuance of EV Certificates, OWGTM SHALL verify (using reliable sources disclosed as per the introduction of this section 3.2) the following: - The Applicant's legal existence and identity, - The Applicant's physical existence (business presence at a physical address), - The Applicant's operational existence (business activity), and - A Verified Method of Communication with the entity to be named as the Subject in the Certificate.

At least in the case of EV Certificates, all identity validation must be corroborated by a second Validation Agent.

In all cases, OWGTM validation practices include the inspection of any documentary evidence or other documents relied upon under this section for alteration or falsification prior to accepting the document as proof of identity or entitlement. Inspection procedures include: 1. verification of the document issuer and issuance date against an authoritative source where available; 2. comparison of document details (name, address, identifiers) against other corroborating sources; 3. visual and electronic checks for signs of alteration (e.g., inconsistent fonts, metadata anomalies, checksum/hash verification for electronic documents); and 4. recording the inspection outcome in the validation record.

Deviations or suspected falsifications SHALL be escalated and handled per the incident handling procedures in Section 8.5.

3.2.2.2 For Personal (S/MIME) Certificates Validation of mailbox authorization or control

General Principles: - OWGTM SHALL verify that Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate or has been authorized by the email account holder to act on the account holder's behalf. - OWGTM does not delegate the verification of mailbox authorization or control. - OWGTM maintains a record of which validation method was used to validate every domain, as indicated in the TLS Certificates CPS or email address in issued Certificates.

Validating authority over mailbox via domain

OWGTM MAY confirm the Applicant has been authorized by the email account holder to act on the account holder's behalf by verifying the entity's control over the domain portion of the Mailbox Address to be used in the Certificate. This method will be used to entitle an Enterprise Registration Authority to issue certificates for the authorized domains.

To perform this verification, OWGTM uses only the approved methods in Section 3.2.2.4 of the TLS Baseline Requirements, as particularized in the section 3.2.2.3 of this CPS.

Validating control over mailbox via email

OWGTM validates the right for the Applicant to use the submitted email address. This is achieved through the delivery via a challenge and response made to the email address submitted during the Certificate application,

as defined in section 3.2.2.6.

In all cases, when an organization name is included in a certificate valid for secure email, the organization validation will follow the steps indicated in section 3.2.2.1 of this document.

CP Identifier	Validation Policy
Standard Personal CertificateAdvanced Personal Certificate,Qualified Personal Certificate Advanced Professional Certificate,Qualified Professional CertificateAdvanced Corporate CertificateQualified Corporate Certificate	Does not Apply: Individual or Organization information will not appear in these certificates The Registration Authority must verify that the Organization exists and that the certificate applicant is authorized to enroll for a certificate in behalf of the Organization name, by means of the authorization of a representative of the same Organization.Any DBA included in a Certificate will be validated using an information source, attestation letter, or reliable form of identification in accordance with section 3.2.2.1 of this document.

3.2.2.3 For TLS Server Certificates

CP Identifier	Validation Policy
DV TLS Certificate	OWGTM confirms the validation of each FQDN in accordance with the CA/Browser Forum Baseline Requirements 3.2.2.4, and in particular using at least one of the methods enumerated below.Currently OWGTM doesn't issue certificates for Onion domains.For each validated FQDN the "TLS Certificate Manager" software used by the OWGTM creates and retains a validation record that includes: (a) the FQDN(s) validated; (b) the specific domain validation method used, related to the version of the Baseline Requirements in force at the moment of validation; (c) date/time of validation; (d) identity of the operator or automated system that performed validation; (e) artifacts evidencing validation (e.g., e-mail headers, DNS TXT contents, HTTP file retrieval response headers and body hash, ACME challenge logs); and (f) any corroboration results from Multi-Perspective Issuance Corroboration (Section 3.2.2.5). Validation records SHALL be retained for at least 2 years after certificate expiry or revocation. In particular, OWGTM will validate the Applicant's right to use or control each domain name that will be listed in the Subject Alternative Name field of a Certificate by using at least one of the following procedures:
OV TLS Certificate	WISeKey will execute the domain validation procedures as required for DV TLS certificates.Additionally, WISeKey will verify:
EV TLS Certificate	WISeKey will execute the domain validation procedures as required for DV and OV TLS certificates.Additionally, WISeKey will do the specific validations mandated by the EV Guidelines issued by the CAB/Forum, as indicated in section 3.2.2.1 of this document.

The list of used validation sources is available at https://wisekey.com/repository. This list is conformed as indicated in the introduction of this section 3.2.

3.2.2.4 For Device Certificates

CP Identifier	Validation Policy
Device Certificate	If the organization name is included in the certificate, the Registration Authority must verify that the Organization exists and that the certificate subscriber is authorized to enroll for a certificate including the Organization name

3.2.2.5 Multi-Perspective Issuance Corroboration (MPIC) CAs in the OWGTM mandatorily implement Multi-Perspective Issuance Corroboration (MPIC) in accordance with CA/Browser Forum Baseline Requirements.

For domain validation and CAA checks that require remote network corroboration, the Primary Network Perspective performs the initial validation and the CA obtains corroborating observations from at least two (2) geographically and topologically distinct remote Network Perspectives (remote vantage points) as required by the Baseline Requirements effective dates. The number of minimum remote perspectives will be increased as per the schedule mandated by the Baseline Requirements.

The CA uses the Quorum Requirements Table in the Baseline Requirements to determine whether the set of observations constitutes corroboration. If the quorum is not achieved per the Baseline Requirements, the CA will not proceed with issuance. The CA retains MPIC logs (primary observation, remote corroboration observations, timestamps, vantage point IDs, and final decision) as part of the validation record. MPIC implementation details (vantage point providers, monitoring frequency, DNSSEC and resolver behavior) are maintained in the CA's operational MPIC procedures (internal document), according to the information published in this document.

The infrastructures supporting the MPIC systems, use Network Hardening mechanisms to mitigate BGP routing incidents in the global Internet routing system for providing internet connectivity to the Network Perspective, and are hosted from an ISO/IEC 27001 certified facility or equivalent security framework independently audited and certified or reported. The MPIC systems are included in the Vulnerability Assessment and Patch Management applied to the rest of the PKI systems.

3.2.2.6 Email Challenge Response Procedure

Unless the domain component of an email address has been already verified for a subscriber, OWGTM verifies the requester's control over the email address by sending a random value via email and then confirming the user entered the random value in our mailbox validation service.

The random value can only be used within a 24-hour timeframe after its generation.

3.2.3 Authentication of individual identity

The same validation practices stated in section 3.2.2.1 will be applied to the authentication of individual identity, considering the following acceptable identity documents: - Government-issued passport
- National identity card / driving license
- Other government ID with photograph

The RA may require additional proof (at its discretion), such as: - Video-based proofing
- Notarized document
- External eID verification (if available)

The following subsections describe the specific practices for each subscriber certificate type.

3.2.3.1 For TLS Certificates

Currently OWGTM doesn't issue TLS "individual-validated" certificates.

For the validation of other individuals participating in the certificate application and management, OWGTM enforces compliance with the CA/B Forum Baseline Requirements and EV Guidelines (see section 3.2.5 of this document).

3.2.3.2 For Personal (S/MIME) Certificates

CP Identifier	Validation Policy
Standard Personal Certificate	**ID Data Verified**:The only verified data is the email address.**Method of Verification**:
Advanced Personal CertificateQualified Personal CertificateAdvanced Professional CertificateQualified Professional Certificate	**ID Data Verified**:Email verification is performed as for the "Standard Personal Certificates".Personal identity data such as name, date of birth, nationality, phone number, etc. Legal entities are required to provide relevant official documentation. Verification of device or other type of entity or object is done with substantially equivalent data. Any names or identity attributes included in the certificate must be verified.**Method of Verification**:May be done through database of identity data that is well-maintained and was created based on face to face or remote verification using official ID documents.**Entities authorized to verify**:
Advanced Corporate CertificateQualified Corporate Certificate	Email verification is performed as for the "Standard Personal Certificates".Individual identity not included in these certificates

Note: Certificate containing the OID for Adobe AATL will be validated according to the rules for Qualified Certificates.

3.2.3.3 For Device Certificates

CP Identifier	Validation Policy
Device Certificate	**ID Data Verified**:Device identity data such as serial number and manufacturer name.**Method of Verification**:May be done through database of identity data that is well- maintained and was created based on face to face or direct verification using official ID documents.If the Extended Key Usage for secure email is set: Bounce back email verification procedure proving access to the email account is accepted.**Entities authorized to verify**:

3.2.4 Non-verified subscriber information

All attributes included in a certificate that are subject to root program or industry regulations must undergo appropriate validation.

3.2.5 Validation of authority

Validation of authority is dependent on the type of Certificate requested and is performed in accordance with the CAB/Forum Requirements and as described below. This process involves a determination of whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a Certificate.

For any Certificate containing Identity Information of an organization, OWGTM SHALL use a Reliable Method of Communication to verify the authorization of the Applicant Representative to send a certificate request, such as determining the liaison of the person sending the request with the Applicant's main business offices, corporate offices, human resource offices, information technology offices.

OWGTM requires that any person participating in any operating process related to certificate generation or status modification is explicitly authorized and the authority verified through a reliable method of communication.

In addition, OWGTM establishes a process that allows an Applicant to specify the individuals who may request Certificates, by facilitating web interfaces that allow the Applicant to maintain a list of authorized accounts.

3.2.6 Criteria for interoperation

A Certification Authority that wishes to interoperate with the OWGTM 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 OWGTM that adheres to this CPS and authorized to issue certain Certificate Types.

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).

3.3.1 Identification and authentication for routine re-key

The certificate subscriber can request a routine re-key by authenticating himself with one of these methods: - Username & Password - A valid digital certificate linked to the user account

The applicable revalidation requirements set by the CA/B Forum for the particular type of certificate will be enforced in the case of reuse of subscriber information (see section 4.2.1).

3.3.2 Identification and authentication for re-key after revocation

The OWGTM 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 request

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. Passwords maybe accepted alternatively.

A Certification Authority may define, that during the enrolment process, a subscriber can create a password that can be used in remote revocation requests, using an on-line procedure communicated to the user when issuing the certificate.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

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

When applicable, CAs operating under the OWGTM must respect the requirements set by the CA/Browser Forum Baseline and EV Requirements.

4.1 Certificate Application

For CA Certificates, before issuing a new certificate for a subordinate Certification Authority OWGTM 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 OWGTM 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 Enrollment process and responsibilities

WISeKey is responsible for ensuring that the identity of each Certificate Applicant is verified in accordance with this CPS prior to the issuance of a Certificate. Applicants are responsible for submitting sufficient information and documentation for the Issuer CA or the RA to perform the required verification of identity prior to issuing a Certificate.

All Certificate Applicants must complete the enrolment process, which may include: - Submit a Certificate application (via our Certificate Management portals), including identity information and agree to the terms of the relevant Subscriber Agreement, presented to the user while sending the request. - Mandatory for TLS Certificates and optional for S/MIME certificates, a valid Certificate Signing Request (CSR) that demonstrates ownership of the private key corresponding to the public key to be included in the certificate. - Make all reasonable efforts to protect the integrity and confidentiality of the Private Key.

For all received requests, the authorized Validation Agent will perform the identity validation tasks as defined in section 3.2. These validation, when referred to validation of domain names or mailboxes, is automated through the Certificate Management portals, and never delegated. The validation of organization information can be automated using official APIs supplied by reliable verification sources.

This process includes the identification of suspicious or potentially dangerous requests, based in automated checks on domain blacklists and previous denied request, marked as suspicious.

4.2 Certificate application processing

This section describes the procedures for processing certificate applications in the OWGTM 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 authorized 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 are delegated to the Registration Authorities operating under the OWGTM.

An authorized Registration Authority Officer will perform these functions. This role can be assumed by: - An accredited person that, on behalf of a Registration Authority, personally executes the identification and authentication functions. - An accredited software application that performs the identification and authentication functions for automated certification procedures. If a Certificate Policy permits such automation it will be stated explicitly in section 4.1.2 of this document. Any accredited software application will execute this function according to sections 3.2.2 and 3.2.3 of this document.

The steps to be executed by the Issuing CA or RA are as follows: - As a first step, the Issuing CA or RA will perform the verifications stipulated in section 3.2. - As a second step, the CA must check the DNS for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, according to the procedure described im section below "CAA processing". - As a third step, the Issuing CA must check the certificate details against a list of previously revoked Certificates and rejected certificate requests to identify suspicious certificate requests.

The Issuing CA can only issue a certificate after having successfully completed the above steps.

CAA processing:

Prior to issuing a TLS or S/MIME certificate including a domain name in the subjectAltName extension, OWGTM checks for and process Certificate Authority Authorization (CAA) records for each DNSName in accordance with RFC 8659. When processing CAA records, OWGTM processes the issue, issuewild, and iodef property tags as specified in RFC 8659; whenever possible, OWGTM will support additional property tags but preventing them to conflict with or supersede the mandatory tags issue, issuewild, and iodef. OWGTM respects the CAA critical flag and will not issue a certificate if an unrecognized property tag is present with the critical flag set. OWGTM platforms log CAA lookup outcomes and document issuance decisions related to CAA records.

If the CA issues a certificate after evaluating CAA records, the issuance occurs within the CAA record's TTL, or 8 hours, whichever is greater. If issuance cannot be completed within that timeframe, OWGTM SHALL re-evaluate the CAA record prior to issuance. The OWGTM platforms log the CAA TTL observed and the issuance timestamp in the validation record and include evidence of compliance with this timing requirement.

WISeKey documents potential issuances that were prevented by a CAA record, and will dispatch reports of such issuance requests to the contact stipulated in the CAA iodef record(s), if present. WISeKey support mailto: and https: URL schemes in the iodef record.

The main identifying CAA domain for WISeKey is 'wisekey.com'. Other accepted domains are 'hightrusted.com', 'certifyid.com' and 'oiste.org'.

In particular for TLS/TLS Certificates:

In compliance with the CA/Browser Forum Baseline Requirements, prior to issuing TLS Digital Certificates, WISeKey performs automated checks for CAA records for each dNSName in the subjectAltName extension of the Digital Certificate to be issued.

In particular for S/MIME Certificates:

In compliance with the CA/Browser Forum Baseline Requirements, prior to issuing S/MIME Digital Certificates, WISeKey performs automated checks for CAA records for each dNSName in the subjectAltName extension of the Digital Certificate to be issued. This practice remained optional until March 15, 2025.

When processing CAA records, WISeKey processes the issuemail property tag as specified in RFC 9495. WISeKey will not issue a Digital Certificate if an unrecognized property is found with the critical flag.

Information reuse policy and applicable deadlines

When performing validations according to section 3.2 of this document, OWGTM may reuse the retained validation records during the following allowed timeframes:

Subject Identity Information shall be: - For S/MIME Certificates: 825 days - For TLS OV Certificates: - Certificates issued before 2026-03-15: 825 days - Certificates issued on or after 2026-03-15: 398 days - For TLS EV Certificates: 398 days

Domain Name and IP Addresses reuse period of SSL/TLS Server Authentication Certificates shall be: - 398 days until March 15, 2026, - effective 2026-03-15, 200 days, - effective 2027-03-15, 100 days, - effective 2029-03-15, 10 days.

Mailbox reuse period of S/MIME Certificates shall be 30 days.

Domain Name reuse period of S/MIME Certificates shall be 398 days.

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 this document.

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

A certificate request will be forwarded to a Certification Authority for its issuance only after the Registration Authority confirms the correctness of the information contained in the request. The OWGTM is not responsible for monitoring, research or confirmation of the correctness of the information contained in a certificate during the intermediate period between its issuance and renewal, unless this period is longer to the current limits established by the CA/Browser Forum in its Baseline Requirements.

4.3.1 CA actions during certificate issuance

A Certification Authority adhering to the OWGTM 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 this document.

4.3.1.1 Linting practices TLS and S/MIME Certificates follow a Linting process to test the technical conformity of each to-be-signed certificate prior to signing it. If the linting results in error, this generates an alert and prevents certificate issuance. Linting warnings also generate alerts and are review to assess the possible impact, but do not necessarily prevent issuance. OWGTM may use a Linting process to test each issued Certificate (e.g. during self-audits).

4.3.1.2 Certificate Transparency For SSL/TLS Certificates that need to be trusted by Application Software Suppliers, OWGTM will be submitted to public Certificate Transparency logs. SCTs returned by logs will be embedded in the certificate or provided via OCSP/stapling as appropriate.

These CT log servers must be qualified and trusted by such Application Software Suppliers.

4.3.2 Notification to subscriber by the CA of issuance of certificate

For CA Certificates, OWGTM notifies directly to the authorized CA responsible.

WISeKey will send, in general, all notifications to the subscriber using email to the address specified in the application process. These notifications should include a digital signature.

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.

Certificate acceptance is understood after the subscriber or his representative performs one or more of the following: - Accepts the “Subscriber Agreement”, which includes the terms and conditions associated with the particular Certificate Policy, and which constitutes formal acceptance of those terms; or - Downloads and/or installs the certificate, making it technically available for usage; or - Doesn’t expressly refuse the certificate once the issuance notification has been sent.

4.4.2 Publication of the certificate by the CA

The CAs operating under the OWGTM 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 this CPS.

4.5 Key pair and certificate usage

The certificates issued by the OWGTM 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 OWGTM PAA.

The specific usages allowed for a private key associated to a certificate type issued in the OWGTM are as summarized in section 2 of this document

4.5.2 Relying party public key and certificate usage

Relying parties must access and use the public key and certificates issued under the OWGTM 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 business decisions.

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

For Subscriber Certificates it is allowed the certificate renewal for the purpose of extending the validity period and always considering the requirements for re-verification periods stipulated in section 4.2.1 of this CPS.

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 OWGTM 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 this document.

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 OWGTM publish all issued certificates as specified in section 2.2 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 this document.

4.8 Certificate modification

The OWGTM does not allow the modification of certificates during their validity period. If the information contained in a certificate cease 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 re-issuance of a new certificate.

4.8.1 Circumstance for certificate modification

No stipulation. Modification is not allowed.

4.8.2 Who may request certificate modification

No stipulation. Modification is not allowed.

4.8.3 Processing certificate modification requests

No stipulation. Modification is not allowed.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation. Modification is not allowed.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation. Modification is not allowed.

4.8.6 Publication of the modified certificate by the CA

No stipulation. Modification is not allowed.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation. Modification is not allowed.

4.9 Certificate revocation and suspension

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

The OWGTM maintains a comprehensive and actionable plan for mass revocation events, performs annual testing of its procedures, and incorporates lessons learned to improve preparedness over time.

Suspension of certificates is not supported.

4.9.1 Circumstances for revocation

All certificate subscribers receiving a digital certificate issued under a Root regulated by this CPS must assume the stipulations contained in this section.

4.9.1.1 Reasons for Revoking a Subscriber Certificate A Certification Authority operating in the OWGTM 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 in the OWGTM 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; 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 TLS 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 in 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; 1. 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; 1. The Issuing CA obtains evidence that the Certificate was misused; 2. 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; 1. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading; 1. 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; 1. 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; 1. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or 1. Revocation is required by the OISTE Foundation.

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 be used for certificate revocation requests is detailed in the "End User Agreement". Individual users will find the appropriate contact and procedure information in the URL http://www.wisekey.com/repository. Certificate subscribers obtaining their certificate from a self-service portal (TLS Manager Portal, Universal Registration Authority, or WISeID Portal) can request the revocation through the same service.

To report suspected Private Key Compromise, Certificate misuse, Certificate mis-issuance, 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@wisekey.com.

For certificate subscribers that seek to obtain general support, the preferred method to communicate with WISeKey is sending an e-mail message to support@wisekey.com.

The common practice for all certificates issued under the OWGTM 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 in the OWGTM.

In particular, processing revocation for TLS Certificates will be performer as required by the CA/Browser Forum.

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 and respecting the deadlines and procedures for problem investigation and reporting set by the CAB/Forum Baseline Requirements and Root Programs.

4.9.6 Revocation checking requirement for relying parties

The OWGTM 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, when available, by using the OWGTM Online Certificate Status Protocol Server (OCSP).

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

4.9.7 CRL issuance frequency

The OISTE Root CAs used by the OWGTM issue a full CRL at least every year, with a typical overlapping period of one week. This CRL will contain the revoked, if any, certificates for OWGTM Policy CAs or Issuing CAs, as appropriate for the hierarchy. A new CRL within twenty-four (24) hours is updated and published after recording a CA Certificate as revoked.

The CRL issuance frequency for Subordinate Certification Authorities is as follows: - The OWGTM Policy CAs issue a full CRL every month, with a typical overlapping period of 3 days. This CRL will contain the revoked, if any, certificates for OWGTM Issuing CAs. New CRL are published immediately if a new subordinated CA is revoked. - The OWGTM Issuing CAs issue a full CRL at least every seven (7) days if all Certificates include an Authority Information Access extension with an id-ad-ocsp accessMethod ("AIA OCSP pointer"); or - four (4) days in all other cases; and will update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

For the specific case of TLS and S/MIME certificates, the OWGTM 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 Issuing Certificate Authorities in the OWGTM may provide an OCSP service that is typically available on a 24x7 basis. The OCSP service availability is generally not available for low assurance certificates, as some types of device or personal certificates.

The URL used to access this service is included in the "AIA extension" in all issued certificates.

For certain Certificates the Issuing CA could publish additional on-line services, web-based or others. Such additional services are stipulated in the appropriate End User Agreement.

In particular for TLS and Code Signing certificates, OWGTM will ensure compliance with the applicable Baseline and/or Extended Validation requirements from the CA/Browser Forum, meaning that CRLs and OCSP are available 24/7 to anyone.

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. This service is made available in compliance with the RFC 6960 and other applicable standards and regulations.

Relying parties are requested to always check the validity of the certificate on which they rely, as stipulated in section 4.9.6.

4.9.11 Other forms of revocation advertisements available

No stipulations.

4.9.12 Special requirements re key compromise

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

In particular for TLS and S/MIME 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 any certificate in scope of the Baseline Requirements, and therefore not allowed for any certificate chaining to an OISTE Root recognized for TLS/TLS or S/MIME certificates.

4.9.14 Who can request suspension

No stipulation. Suspension is not available for publicly trusted certificates.

4.9.15 Procedure for suspension request

No stipulation. Suspension is not available for publicly trusted certificates.

4.9.16 Limits on suspension period

No stipulation. Suspension is not available for publicly trusted certificates.

4.10 Certificate status services

Any CA operating in the OWGTM must provide a highly available and reliable service for checking the status of all certificates issued under its Trust Model.

4.10.1 Operational characteristics

Certificate Status Services are accessible through HTTP servers owned by the OWGTM 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 OWGTM.

4.12 Key escrow and recovery

Key escrow is not permitted for TLS Certificates.

4.12.1 Key escrow and recovery policy and practices

All CA providing Key Escrow services for Personal Certificates are required to: - Notify Subscribers that their Private Keys are escrowed; - Protect escrowed keys from unauthorized disclosure; - Protect any authentication mechanisms that could be used to recover escrowed Private Keys; Release an escrowed key only after making or receiving (as applicable) a properly authorized request for recovery; and - Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key related information, or the facts concerning any key recovery request or process.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This section describes the non-technical security controls used by the participants2 involved in the issuance, publishing and management of keys within the OWGTM. The OWGTM 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 OWGTM web site (http://www.oiste.org/repository).

The OWGTM may allow third parties to host and operate 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 their hierarchies (and related certificate publication and verification services) to WISeKey. - The "Issuing CAs" (and related certificate publication and verification services) are hosted and operated by WISeKey (except for the cases of technically-constrained CAs, which could be hosted by their owners). These participants are allowed to delegate the hosting and operation of CAs 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 WISeKey. Registration Authorities are not allowed to delegate their operations to other parties without the approval and direct supervision of WISeKey.

OWGTM's CA infrastructure, certificate systems, network boundary controls and security support systems are managed in accordance with the CA/Browser Forum Network and Certificate System Security Requirements (NCSSR), in its latest version, and the controls described in this CPS.

5.1 Physical controls

This section describes the physical controls on facilities housing OWGTM components.

5.1.1 Site location and construction

The OWGTM 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.

OWGTM secure datacenters and all copies (online and offline) of CA root and intermediate private keys are located in Switzerland.

5.1.2 Physical access

The OWGTM 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.

5.1.3 Power and air conditioning

The OWGTM Secure Datacenter implements power and air conditioning systems sufficiently dimensioned to accommodate the operating needs, protected by Uninterruptible Power Supply units (UPS) and backup power generators.

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, magnetic or electronic media and paper containing any information generated during OWGTM 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 Off-site backup

OWGTM 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.

All key backups are stored on HSM devices meeting FIPS 140 Level 3 criteria.

5.2 Procedural controls

The information systems and services incorporated in the OWGTM are operated in a secure manner, following a set of predefined procedures that are enforced by the OWGTM 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 OWGTM components and operations.

5.2.1 Trusted roles

The OWGTM 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 Administrator - Certification Authority Operator - Registration Authority Administrator - Registration Authority Operator with Vetting attributions (AKA Validation Agent or Specialist) - Registration Authority Operator without Vetting attributions - Systems Administrator - Security Administrator - Policy Approval Authority Member

Each Trusted Role has its responsibilities, privileges, and access documented. Any account capable of authenticating to or accessing CA Infrastructure or Network Boundary Controls is reviewed at a minimum frequency of every three (3) months.

Each Trusted Role is assigned responsibilities, privileges, and access in a manner consistent with: - the Principle of Least Privilege; and - the Principle of Separation of Duties.

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

Root and Issuing CA key generation, activation, backup, and recovery, and also entering areas hosting Root CA systems, require at least two people in Trusted Roles to be present.

Validation of EV certificates require the participation of at least two different Validation Agents.

5.2.3 Identification and authentication for each role

All the persons assuming a role in the OWGTM systems4 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 OWGTM's systems and services systems is typically enforced using two factor authentication that usually includes biometrics.

5.2.4 Roles requiring separation of duties

Individuals are specifically designated to one or more of the roles defined in Section 5.2.1.

OWGTM enforces the separation of roles whenever required to avoid conflict of interests or undermining of security levels.

5.3 Personnel controls

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

5.3.1 Qualifications, experience, and clearance requirements

Personnel acting directly or indirectly for the OWGTM 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 OWGTM 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 OWGTM, 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.

In particular, OWGTM enforces specific practices for the training, examination, and record-keeping of the Validation Specialists. We define a role of Validation Specialist for personnel who perform identity and domain validations. Prior to performing Validation Specialist duties, the CA SHALL document that each Validation Specialist: - has completed CA-provided training covering the Baseline Requirements, CP/CPS procedures, the CA's validation tools, and the handling of suspicious requests; - has passed the CA's validation examination with a passing score defined by the CA; and - is formally authorized in writing to perform validations.

OWGTM maintains training and examination records for each Validation Specialist, including training content version, date completed, exam results, and authorization records. Validation Specialists SHALL receive periodic refresher training at least annually and whenever the Baseline Requirements or internal procedures are updated. OWGTM retains training and personnel qualification records for the duration of employment plus 3 years.

5.3.4 Retraining frequency and requirements

Retraining sessions are performed at least annually and 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 OWGTM will undertake necessary disciplinary actions. Any action that (intentionally or unintentionally) contravenes the Certification Practice Statement.

Upon detection of an unauthorized action the OWGTM will initiate an investigation process. During this process the involved persons will be prevented from obtaining access to OWGTM 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 OWGTM 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.

Training requirements for contractors must meet the same requirements that the applied to WISeKey employees assigned to the same role.

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 OWGTM are provided access, as required for their role, to the following information: - Certification Practices Statement - Certificate Policies - Privacy Policy - Security Policy - Organization chart and assigned functions and responsibilities - Operational procedures - Incident response procedures - Applicable standards or requirements (e.g. CAB/F or Root Programs requirements)

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 OWGTM.

5.4.1 Types of events recorded

OWGTM PKI systems record at least the following events:

- CA certificate and key lifecycle events, including:
  1. Key generation, backup, storage, recovery, archival, and destruction;
  2. Certificate requests, renewal, and re-key requests, and revocation;
  3. Approval and rejection of certificate requests;
  4. Cryptographic device lifecycle management events;
  5. Generation of Certificate Revocation Lists;
  6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10); and
  7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
- Subscriber Certificate lifecycle management events, including:
  1. Certificate requests, renewal, and re-key requests, and revocation;
  2. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
  3. Approval and rejection of certificate requests;
  4. Issuance of Certificates;
  5. Generation of Certificate Revocation Lists; and
  6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).
  7. Multi-Perspective Issuance Corroboration attempts from each Network Perspective, minimally recording the following information:
     - an identifier that uniquely identifies the Network Perspective used;
     - the attempted domain name and/or IP address; and
     - the result of the attempt (e.g., "domain validation pass/fail", "CAA permission/prohibition").
  8. Multi-Perspective Issuance Corroboration quorum results for each attempted domain name or IP address represented in a Certificate request (i.e., "3/4" which should be interpreted as "Three (3) out of four (4) attempted Network Perspectives corroborated the determinations made by the Primary Network Perspective).
- Security events, including:
  1. Successful and unsuccessful PKI system access attempts;
  2. PKI and security system actions performed;
  3. Security profile changes;
  4. Installation, update and removal of software on a Certificate System;
  5. System crashes, hardware failures, and other anomalies;
  6. Relevant router and firewall activities (as described in Section 5.4.1.1); and
  7. Entries to and exits from the CA facility.

Log records MUST include at least the following elements: - Date and time of event; - Identity of the person making the journal record (when applicable); and - Description of the event.

5.4.1.1 Router and firewall activities logs Logging of router and firewall activities necessary to meet the CAB/Forum Baseline Requirements of Section 5.4.1, Subsection 3.6, and at a minimum include: - Successful and unsuccessful login attempts to routers and firewalls; and - Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications;

and - Logging of all changes made to firewall rules, including additions, modifications, and deletions; and - Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

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

OWGTM and each Delegated Third Party SHALL retain, for at least two (2) years: 1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1) after the later occurrence of: - the destruction of the CA Private Key; or - the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key; 2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1) after the expiration of the Subscriber Certificate; 3. Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

5.4.4 Protection of audit log

Audit logs, whether in production or archived, are protected from modification, substitution, or unauthorized destruction. All archived 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 OWGTM auditor and the OWGTM 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 OWGTM 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

OWGTM maintains a documented vulnerability management program: critical vulnerabilities should be remediated within 3 days (or mitigated), with monthly patch/scan cycles and annual third-party penetration tests.

OWGTM executes regular vulnerability assessment by monitoring the activity logs, at least with a quarterly frequency. 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 OWGTM will inform the involved parties and records of such an event and its cause will be kept for future reference.

In particular, OWGTM performs an annual Risk Assessment that: 1. identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management processes; 2. assesses the likelihood and potential damage caused by these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management processes; and 3. assesses the adequacy of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Periodic Penetration Tests, at least annually, and quarterly Vulnerability Scans are conducted by a highly skilled security team with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.

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

5.5 Records archival

This section includes the stipulations regarding record archival and 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 OWGTM 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 two years after the validity of the involved certificates, or as stipulated by the CAB/Forum applicable requirements, whatever is greater.

For the particular case of TLS and EV certificates, The CA must ensure the retention period 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 OWGTM 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 OWGTM 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 OWGTM.

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

OWGTM 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 OWGTM 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 OWGTM. 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 OWGTM 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.

In the event of detected or suspected compromise of CA Infrastructure, OWGTM's incident response procedures comply with the CABF NCSSR requirements for alerting, response time, root-cause analysis, containment and remediation.

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

5.7.1.1 Incident Response and Disaster Recovery Plans OWGTM documents an Incident Response Plan and a Disaster Recovery Plan.

OWGTM documents a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. OWGTM makes its business continuity plan and security plans available to our auditors upon request. OWGTM annually tests, reviews, and updates these procedures.

The business continuity plan includes: 1. The conditions for activating the plan, 1. Emergency procedures, 1. Fallback procedures, 1. Resumption procedures, 1. A maintenance schedule for the plan; 1. Awareness and education requirements; 1. The responsibilities of the individuals; 1. Recovery time objective (RTO); 1. Regular testing of contingency plans. 1. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes 1. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; 1. What constitutes an acceptable system outage and recovery time 1. How frequently backup copies of essential business information and software are taken; 1. The distance of recovery facilities to the CA's main site; and 1. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

Compromise Notification
In the event of key compromise (CA root, subordinate, or certificate-subscriber key), the CA **must**: 1. Immediately revoke affected certificates.
2. Notify relevant stakeholders (subscribers, RAs, responding authorities) per defined procedures.
3. Report to browser or trust-store maintainers, if relevant, according to their programs / requirements.
4. Retain forensic evidence (logs, access records) for investigation.

Post-Incident Review
After any incident, the CA must conduct a **post-incident review**, document lessons learned, update the IR plan, and remediate root causes.

5.7.1.2. Mass Revocation Plans As required by Root Programs and the CABF Baseline Requirements, OWGTM maintains a mass revocation plan to ensure a rapid, consistent, and reliable response to large-scale certificate revocation events. The Mass Revocation Plan is tested, reviewed, and updated at least annually.

Mass revocation provisions include: 1. Activation criteria – specific, objective, and measurable thresholds at which the mass revocation plan is triggered based on the CA's risk profile, issuance volumes, and operational capabilities; 1. Customer contact information – how subscriber and customer contact details are stored, maintained, and kept up to date; 1. Automation points – processes that are automated or could be automated, and those processes that require manual intervention; 1. Targets and timelines – for incident triage, revocation

initiation, certificate replacement, and post-event review; 1. Subscriber notification methods – mechanisms for notifying impacted Subscribers; 1. Role assignments – roles and responsibilities of personnel responsible for initiating, coordinating, and executing the plan; 1. Training and education – training, awareness, and readiness activities for personnel responsible for, or supporting, the plan; 1. Plan testing – annual operational testing to assess readiness and demonstrate implementation feasibility, using one or more of tabletop exercises, simulations, parallel testing, or controlled test environments that DO NOT involve the revocation of active Subscriber Certificates; and 1. Post-test analysis and update schedule – how lessons learned from testing or live incidents are incorporated into the plan, and how often it is reviewed and updated.

The external audit on the Mass Revocation Plan is included in the scope of the annual Webtrust audit for TLS Baseline Requirements.

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 OWGTM 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 OWGTM 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 OWGTM's main facilities, and any services that are provided from these, the OWGTM 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 OWGTM 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 OWGTM 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 OWGTM. - 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 OWGTM 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 OWGTM5. The OWGTM 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 OWGTM, 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

6.1.1.1 CA Key Pair Generation Key Pairs of Certification Authorities operating in the OWGTM 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 auditor6. - 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 OWGTM are generated in hardware security modules (HSM) accredited under the standards specified in section 6.2.1.

All CA private keys are generated and protected within validated HSMs (FIPS 140-2 Level 3 or equivalent). CA HSM administrative access requires split knowledge and multi-person authentication.

Key pairs for the Policy and Issuing Certification Authorities in the OWGTM 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.

For Subscriber Certificates, unless otherwise noted in this CPS, Subscriber is solely responsible for the generation of the Key Pair appropriate to the Certificate type being applied for. The OWGTM explicitly disallows server-side generation and storage of keys for TLS Certificates.

6.1.1.2 RA Key Pair Generation No stipulation.

6.1.1.3 Subscriber Key Pair Generation OWGTM will reject a certificate request if one or more of the following conditions are met: 1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6; 1. There is clear evidence that the specific method used to generate the Private Key was flawed; 1. The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise; 1. The CA has previously been notified that the Applicant's Private Key has suffered a Key Compromise using the CA's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12; 1. The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the following precautions SHALL be implemented: 1. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), the CA SHALL reject all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, the CA SHALL reject Debian weak keys. 1. In the case of ROCA vulnerability, the CA SHALL reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent. 1. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), the CA SHALL reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

If the Subscriber Certificate will contain an extKeyUsage extension containing either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280], OWGTM will generate a Key Pair on behalf of a Subscriber, and will not accept a certificate request using a Key Pair previously generated by the CA.

6.1.2 Private key delivery to subscriber

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

If the specific subscriber certificate type allows the generation of the private key by the Registration Authority, the usage of password-protected encrypted software files, or smart-cards or other valid crypto-tokens is accepted.

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

6.1.3 Public key delivery to certificate issuer

Public keys generated by, or for, the end-entities are sent to the Certification Authority through secure channels using the OWGTM Registration Authorities, as part of a certificate request in acceptable formats, such as PKCS#10 or other standard CSR format.

6.1.4 CA public key delivery to relying parties

The public keys of all Certification Authorities operating under the OWGTM Trust Model are included in the corresponding certificate and published in public repositories such as CCADB.

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

6.1.5 Key sizes

The OWGTM enforces the use of minimum length 2048-bit RSA (key length must divisible by 8) and ECC NIST P-256, P-384 or P-521 for key pairs at all levels of the hierarchy.

CAs that generate Certificates and CRLs under this policy SHOULD use the SHA-256, or SHA-384 hash algorithm when generating RSA digital signatures. ECDSA signatures on Certificates and CRLs SHOULD be generated using SHA-256, SHA-384 or SHA-512, as appropriate for the key length.

6.1.6 Public key parameters generation and quality checking

The algorithm used in the OWGTM for key generation is RSA or ECDSA.

RSA: OWGTM confirms that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 2^16 + 1 and 2^256 - 1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

ECDSA: OWGTM SHOULD confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

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.

Private Keys corresponding to Root Certificates must not be used to sign Certificates except in the following cases: - Self-signed Certificates to represent the Root CA itself; - Certificates for Subordinate CAs and Cross Certificates; - Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and - Certificates for OCSP Response verification.

All subscriber certificates issued in the OWGTM contain the "KEY USAGE" and "EXTENDED KEY USAGE" attributes, as defined by the X.509v3 standard. More information is available in section 7 of this document.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The OWGTM 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 OWGTM are required to use Hardware Security Modules, at least compliant with FIPS 140-2 Level 2 for PKI components (Level 3 for CA components).

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 OWGTM 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 section 4.1.2. In particular, backup of private keys for TLS Certificates is nor allowed.

6.2.5 Private key archival

The CA shall not provide key archival services to subscribers. Private keys of expired or revoked CAs may be archived by being left in HSM or their backup.

6.2.6 Private key transfer into or from a cryptographic module

For Certification Authorities operating under the OWGTM 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

All CA Private Keys are stored on a cryptographic module which has been evaluated to at least FIPS 140-2 level 3, FIPS 140-3 level 3, or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.

6.2.8 Method of activating private key

The private key in Certification Authorities in the OWGTM 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 (smart-card 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 OWGTM 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
Other OWGTM Roots	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 appropriate for the certificate type (See Appendix D, Certificate Profiles)

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.

The operational period of CA and subscriber certificates are included in Appendix D, Certificate Profiles and can be restricted by the applicable regulations, such as: - CA/B Forum Baseline Requirements for TLS Certificates - CA/B Forum Baseline Requirements for S/MIME Certificates - Particular provisions of certain Root Programs

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.

End entity activation data, is only stipulated for hardware-based private-keys. In particular: - Private Keys for RA and Qualified Certificates, if protected in a hardware device, will require the usage of a password or PIN code of eight or more characters in order to activate the hardware device where the key is stored. - Private Keys for "Standard Personal Certificates" can be generated and installed without using a password, although this is discouraged.

Private Keys for other types of certificates must be generated after the subscriber is properly authenticated in the system where the keys are being created. An accepted method is the use of reasonably secure passwords to access the RA User Interface.

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 authorized personnel involved in the OWGTM operations and only disclosed to accredited external parties for auditing purposes.

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

In particular, OWGTM SHALL implement access controls, monitoring, logging, alerting, change management, vulnerability management and operational security in accordance with the latest version of the CABF NCSSR and shall retain evidence of compliance with the requirements contained therein.

6.5.1 Specific computer security technical requirements

OWGTM 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: - Maintaining Root CA Systems in a high security zone and in an offline state or Air-Gapped from other networks - Strong password policies, enforcing multi-factor authentication for all accounts capable of directly causing certificate issuance - Granting administration access to Certificate Systems only to persons acting in Trusted Roles and requiring their

accountability for the Certificate System's security - Removing or disabling all accounts, applications, services, protocols, and ports that are not used in operations - Constant improvement of administration and operating procedures - Physical isolation of confidential systems - Antivirus and anti-malware detection systems - Periodic internal security reviews

Workstations are configured in a manner that prevents continued access to the Workstation after a set period of inactivity, for example by automatically logging off active users.

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

No stipulation.

6.6 Life cycle technical controls

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.

In particular, regarding Linting software, we monitor for updated versions of any third party Linting software utilized in the CA service, and plan for updates no later than three (3) months from the release of the update. When appropriate, we perform Linting on the corpus of its unexpired, un-revoked Subscriber Certificates whenever after an update the Linting software.

6.6.2 Security management controls

The OWGTM 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

OWGTM establishes and maintains a change management process which is aligned with the CABF NCSSR: 1. documented comprehensively; 1. authoritative for: - all personnel in Trusted Roles; - management of Network Boundary Controls; and - management of CA Infrastructure; 1. reviewed annually; 1. updated as needed; and 1. approved: - with each update; - prior to going into effect; and - by personnel in applicable Trusted Roles.

6.7 Network security controls

The OWGTM enforces the adoption of effective controls to minimize any risk related to Network Security.

OWGTM infrastructures are protected in accordance with the CA/Browser Forum Network and Certificate System Security Requirements (NCSSR), in its latest version.

These protections include: - Periodic vulnerability scans - Effective network segmentation through firewalls systems and other controls - Detection and prevention measures to guard against viruses and malicious software; and - Monitoring controls for health and any abnormal activity - System security patches management - Managing logical access permissions in accordance with a formal procedure - Enforcing multi-factor authentication - Monitoring the configuration of access permissions - Regular training of personnel in trusted roles

Vulnerability scans of networks are performed at least quarterly. Independent penetration tests are performed by external auditors at least annually. Remediation measures are implemented based on severity, as follows: - Critical severity vulnerabilities are addressed within 96 hours - High severity vulnerabilities are addressed within 10 days - Medium or lower severity vulnerabilities are addressed within 60 days, where feasible.

Exceptions are documented, assessed for risk, and recorded.

In particular, the server used for the OWGTM 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.

When allowed, remote connections are enabled in accordance with the CABF NCSSR.

The detailed information about these controls is classified and only made available for external auditors after the appropriate authorization process.

6.8 Time-stamping

The OWGTM 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, CRL, AND OCSP PROFILES

All certificates issued under the OWGTM 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").

7.1 Certificate profile

The OWGTM defines different certificate profiles corresponding to the allowed certificate types issued under the different hierarchies.

The different profiles are mainly differentiated by the appropriate combination of values in the "Key Usage", "Extended Key Usage" and/or the use of particular Policy Identifiers. This combination of values can imply that the certificate is mandatorily subject to requirements stipulated by the CA/B Forum and/or Root Programs, that take precedence over stipulations in this document. In particular: - Server Authentication Certificates are subject to the CABF Baseline Requirements and (if applicable) EV Guidelines regulating these types of certificates. - Secure Email Certificates are subject to the CABF Baseline Requirements for S/MIME Certificates.

The OWGTM must ensure that he certificate profiles are aligned with the above requirements.

The details of the relevant certificate profiles is included in the Appendix D, Certificate Profiles.

7.1.1 Version number(s)

All certificates in the OWGTM conform to X.509 Version 3.

7.1.2 Certificate extensions

For subordinate CA Certificates, OWGTM 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 TLS and S/MIME certificates the CA SHALL ensure compliance with the Baseline Requirements 7.1.2 and related sections. These details can be found in the Appendix D, Certificate Profiles.

7.1.3 Algorithm object identifiers

For the Root CA and subordinate CA certificates, the used algorithms are: - sha-1WithRSAEncryption (deprecated, not allowed for new issuances) - sha256WithRSAEncryption, sha384WithRSAEncryption, sha512WithRSAEncryption - ecdsa-with-sha512/384/256

For subscriber certificates, only the above algorithms permitted by the applicable requirements are allowed (see Appendix D, Certificate Profiles).

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.

7.1.5 Name constraints

OWGTM 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).

Domain name constraints can be also applied when using the Managed PKI RA Interface for Certificate Requests for corporations having access to a dedicated Registration Authority.

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 OWGTM and listed in the Appendix C, "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

Unless disallowed by the applicable requirements, certificates may contain information in the Certificate Policy extension.

7.1.9 Processing semantics for the critical Certificate Policies extension

The "Certificate Policy" extension identifies the Policy that the OWGTM assigned explicitly with a certificate policy. 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 OWGTM 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 OWGTM.

7.2.2 CRL 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

The usage of the "Reason Code" is appropriately communicated in the Subscriber Agreement, according to the table below. End users being able to select the reason when revoking their certificates, must abide to use the appropriate reason.

RFC 5280 reasonCode	Value	Description
unspecified	0	Represented by the omission of a reasonCode. MUST be omitted if the CRL entry is for a Certificate not technically capable of causing issuance unless the CRL entry is for a Subscriber Certificate subject to these Requirements revoked prior to July 15, 2023.
keyCompromise	1	Indicates that it is known or suspected that the Subscriber's Private Key has been compromised.
affiliationChanged	3	Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.
superseded	4	Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable 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, or the CA has revoked the Certificate for compliance reasons such as the Certificate not complying with the Baseline Requirements or the CA's CP or CPS.
cessationOfOperation	5	Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or the Subscriber no longer owns or controls the Domain Name in the Certificate prior to expiration.

RFC 5280 reasonCode	Value	Description
certificateHold	6	MUST NOT be included if the CRL entry is for (1) a Certificate subject to these Requirements, or (2) a Certificate not subject to these Requirements and was either (A) issued on-or-after 2020-09-30 or (B) has a notBefore on-or-after 2020-09-30.
privilegeWithdrawn	9	Indicates that there has been a subscriber-side infraction not resulting in keyCompromise, such as providing misleading information in the Certificate Request or failing to uphold material obligations under the Subscriber Agreement or Terms of Use.

In particular, the use of the reason "keyCompromise", when the revocation is done by the CA or RA, is regulated as described in section 4.9.12.

7.3 OCSP profile

In general, the status of all certificates in the OWGTM, except if indicated in the appropriate Certificate Policy, may be validated by sending requests compliant with RFC 6960 and/or RFC 5019.

OWGTM ensures compliance with any applicable requirement from the CA/Browser Forum in terms of OCSP implementation for server authentication certificates. In particular, the CRLReason indicated MUST contain a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 Version number(s)

OWGTM provides OCSP responses in accordance with industry standards.

7.3.2 OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

OWGTM 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.

OWGTM shall carry out internal and external audits, risk assessments, system inventories, and reviews of its CA infrastructure, network boundary controls and Certificate Systems in alignment with the NCSSR and other applicable requirements. OWGTM shall publish (or retain in records) the timeframes and policies referenced in those requirements.

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 TLS certificates, the OWGTM 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 OWGTM at an organization level.

8.3 Assessor's relationship to assessed entity

The OWGTM 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 OWGTM establishes the need to audit and accreditation. - The Root CA, Policy CAs and Issuing CAs owned or operated by WISeKey. These services are audited against the different WebTrust criteria and commonly accepted industry accreditation standards. - 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 OWGTM 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 OWGTM 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 OWGTM could decide to temporarily suspend the activities of the affected systems or services until the deficiency is solved.

OWGTM will ensure that deficiencies are publicly disclosed via the appropriate channels (i.e. by opening a Bugzilla incident report), whenever required by the CAB/Forum or Root Program requirements.

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 - OWGTM Policy Approval Authority - Root Programs, in the case of need - 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 OWGTM and Issuing Repository.

8.7 Self-Audits

In compliance with the CABF Requirements, OWGTM performs a quarterly internal audit of at least a random 3% of certificates issued during the period. This audit includes linting of the selected certificates.

Additionally, OWGTM performs self-assessments as required by the root programs and publishes the results in the CCADB platform.

Results are saved and provided to auditors upon request.

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.

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 OWGTM 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

OWGTM 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

OWGTM 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 OWGTM 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 OWGTM 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 stipulation.

9.2.3 Insurance or warranty coverage for end-entities

The maximum liability per subscriber certificate issued under the OWGTM is to be established in the applicable Subscriber Agreement published by the Issuing CA.

9.3 Confidentiality of business information

In general, an Issuing CA under the OWGTM 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 OWGTM 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 "STRICTLY 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 OWGTM 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 OWGTM must publish their own Privacy Policy and communicate it adequately to the certificate subscribers. 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

WISeKey publishes the Privacy Policy and other related materials in https://www.wisekey.com/repository.

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 OWGTM ensures the compliance of the legal obligations for Certification Authorities, Registration Authorities and other entities operating under the OWGTM 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 OWGTM 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 OWGTM 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

OWGTM 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 OWGTM 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 OWGTM, 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 OWGTM 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 OWGTM 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. In the case of key compromise, the Subscriber is bound to communicate the situation as stipulated in this CPS and the Subscriber Agreement. - 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.

OWGTM implements a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. The CA MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

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 stipulation.

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 other documents 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, OWGTM'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 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 OWGTM 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 CP/CPS 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 OWGTM 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 OWGTM 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 OWGTM 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 OWGTM 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 provisions

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

he CP, the CPS and the operations of the OWGTM 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 OWGTM 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.

If a Law in any jurisdiction where OWGTM operates or issues certificates conflicts with a Baseline Requirement, we may modify our internal processes only to the minimum extent necessary to comply with that Law. Prior to issuing any certificate under such a modified process, we will publish in this Section 9.16.3: - a detailed reference to the Law (statute/regulation/order, jurisdiction and date); - a description of the specific Baseline Requirement(s) affected; and - the precise modification(s) implemented by the CA.

When required, OWGTM retains documentation supporting the legal determination and will notify the applicable Root Programs and auditors as required by those programs.

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 stipulation.

Appendix A: Glossary

Acronyms

Acronym	Description
AATL	Adobe Approved Trust List
CA	Certificate Authority or Certification Authority
CAA	Certification Authority Authorization
CAB or CA/B	"CA/Browser" as in "CAB Forum"
CMS	Certificate Management System
CP	Certificate Policy
CPS	Certification Practice Statement

Acronym	Description
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DBA	Doing Business As (also known as “Trading As”)
DNS	Domain Name Service
DV	Domain Validated
ETSI	European Telecommunications Standards Institute EU
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
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
IETF	Internet Engineering Task Force
IGTF	International Grid Trust Federation
ITU	International Telecommunication Union
IV	Individual Validated
NCSSR	CA/Browser Forum’s“Network and Certificate System Security Requirements
MICS	Member-Integrated Credential Service (IGTF)
MPIC	Multi-Perspective Issuance Corroboration
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validated
PAA	Policy Approval Authority
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
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
TLS	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

Definitions

Definition	Description
Applicant	An entity applying for a Certificate.
Attestation Letter	A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
Certification Authority Authorization or CAA	From RFC 9495: "The Certification Authority Authorization (CAA) DNS resource record (RR) provides a mechanism for domains to express the allowed set of Certification Authorities that are authorized to issue certificates for the domain." CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue.
CAB Forum	CA/Browser Forum, https://cabforum.org
Certificate	An electronic document, conformant to X.509v3, digitally signed by a Certificate Authority, that binds a Public Key to an identity.
Certificate Approver	Defined in the EV Guidelines.
Certificate Management System	The keys, software and hardware used to verify Certificate Data, maintain a Repository, and issue and revoke Certificates.
Certificate Management Process	The policies, practices, and procedures governing the use of the Certificate Management System
Certificate Requester	Defined in the EV Guidelines.
Contract Signer	Defined in the EV Guidelines.
Domain Name	An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.
EV Guidelines	As defined by the CA/B Forum at https://cabforum.org/working-groups/server/extended-validation/about/
Hardware Crypto Module	A tamper-resistant device, with a cryptography processor, used for the specific purpose of protecting the lifecycle of cryptographic keys (generating, managing, processing, and storing).
Internal Name	A string of characters (not an IP address) in a Common Name or Subject
Alternative Name	Field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.
IP Address	A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.
Issuer CA	Any CA issuing Certificates under this CP/CPS
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
Key Pair	A Private Key and associated Public Key.
Linting	A process in which the content of digitally signed data such as a Pre-certificate [RFC 6962], Certificate, tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in the applicable Requirements.

Definition	Description
Mailbox address	An Email Address as specified in Section 4.1.2 of RFC 5321 and amended by Section 3.2 of RFC 6532, with no additional padding or structure.
OCSP Responder	An online software application operated under the authority of the OWGTM for processing certificate status requests.
Onion Domain Name	A Fully Qualified Domain Name ending with the RFC 7686 ".onion".
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Relying Party	An entity that relies upon either the information contained within a Certificate or a time-stamp token.
Relying Party Agreement	An agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate.
Reserved IP Address	An IPv4 or IPv6 address that is contained in the address block of any entry in either of the appropriate IANA registries.
Signing Service	An organization that generates the Key Pair and securely manages the Private Key associate with a Code Signing Certificate on behalf of a Subscriber.
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the Subject commonName field.
Subscriber	Either the entity identified as the subject in the Certificate.
Subscriber Agreement	An agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.
Suspect Code	Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, code that compromises user security and/or code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the Platforms on which it executes
WebTrust	The current version of CPA Canada's WebTrust Program for Certification Authorities.
WHOIS	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol, the Registry Data Access Protocol, or an HTTPS website.

Appendix B: CA Hierarchies

Legacy OISTE Root "Generation A"

Root Information

Subject Name	Fingerprint	Audit scope
CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH	41C923866AB4CAD6B7AD578081582E020D[illegible]7D7F5	S/MIME Certificates

Subordinate CA Information

Subject Name	Fingerprint	Allowed usage
CN=WISeKey CertifyID Advanced Services CA 4, OU=International, OU=Copyright (c) 2016 WISeKey SA, O=WISeKey, C=CH	41144BD4174C3152E1CA526F77D9F9C[illegible]64B5101D3	Email, Document Signing

Legacy OISTE Root "Generation B"

Root Information

Subject Name	Fingerprint	Audit scope
CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	6B9C08E86EB0F767CFAD65CD98B62149[illegible]86BD6	S/MIME Certificates

Subordinate CA Information

Subject Name	Fingerprint	Allowed usage
CN=WISeKey CertifyID SSL GB CA 2, O=WISeKey, C=CH	C8A610BA9417770D2C02DE22BCA8C56A[illegible]DDB7CFC	TLS/SSL Certificates
CN=TuringSign RSA Secure CA, O=Turing Crypto GmbH, C=DE	12976558B68E8E1EAA79A629A8E4D17[illegible]D156	TLS/SSL Certificates
CN=TuringSign ECC Secure CA, O=Turing Crypto GmbH, C=DE	1937B9BF662FB578407B77AB87D8D6[illegible]1952B19C80	TLS/SSL Certificates
CN=TuringSign RSA Secure CA 2, O=TuringSign Global SA, C=CH	A6F9C967EB8AA9283A1CA649B87B764[illegible]98CF6	TLS/SSL Certificates
CN=TuringSign ECC Secure CA 2, TuringSign Global SA, C=CH	A5F41EDF8D6E045FF3FEED676650CE0[illegible]1695C47AA9DFF11D5C5	TLS/SSL Certificates
CN=WISeKey CertifyID Personal GB CA 3, O=WISeKey, C=CH	E5937790AA6915755C9A532B10C961[illegible]A3786F5	Email, Document Signing
CN=WISeKey CertifyID Personal GB CA 4, O=WISeKey, C=CH	8D45BF32C041A7EE46325F06AE604FA[illegible]A56FFB8	Email

Legacy OISTE Root "Generation C"

Root Information

Subject Name	Fingerprint	Audit scope
CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	8560F91C3624DABA9570B5FEA0DBE36FF11A8323BEC28A [illegible]	[illegible]

Subordinate CA Information

Subject Name	Fingerprint	Allowed usage
CN=WISeKey CertifyID Advanced GC CA 1, O=WISeKey, C=CH	387D496B92202D4C443CD94FF42DA17 [illegible]	[illegible]
CN=WISeKey CertifyID SSL GC CA 1, O=WISeKey, C=CH	B05E05CFCBF81813EC30FA3F74920AA [illegible]	[illegible]

New OISTE Root for Client/Personal certificates (ECC) "Generation 1"

Root Information

Subject Name	Fingerprint	Audit scope
CN=OISTE Client Root ECC G1, O=OISTE Foundation, C=CH	D9A32485A8CCA85539CEF12FFFFF711 [illegible]	[illegible]

Subordinate CA Information

Subject Name	Fingerprint	Allowed usage
CN=WISeKey CertifyID Client ECC CA 1, O=WISeKey, C=CH	1F5233119B894DB95B4A3737397366 [illegible]	[illegible] Email, Document Signing

New OISTE Root for Client/Personal certificates (RSA) "Generation 1"

Root Information

Subject Name	Fingerprint	Audit scope
CN=OISTE Client Root RSA G1, O=OISTE Foundation, C=CH	D02A0F994A868C66395F2E7A880DF50 [illegible]	[illegible]

Subordinate CA Information

Subject Name	Fingerprint	Allowed usage
CN=WISeKey CertifyID Client RSA CA 1, O=WISeKey, C=CH	41F8755AEE782FF08D8EBB579ABC330 [illegible]	[illegible] Email, Document Signing

New OISTE Root for TLS Server certificates (ECC) "Generation 1"

Root Information

Subject Name	Fingerprint	Audit scope
CN=OISTE Server Root ECC G1, O=OISTE Foundation, C=CH	EEC997C0C30F216F7E3B8B307D2BAE42[illegible]850F49	[illegible]

Subordinate CA Information

Subject Name	Fingerprint	Allowed usage
CN=WISeKey CertifyID Server ECC CA 1, O=WISeKey, C=CH	042FCAA086492C92FB02A82AC957489[illegible]A6901BBB548A8AC88A380	[illegible]

New OISTE Root for TLS Server certificates (RSA) "Generation 1"

Root Information

Subject Name	Fingerprint	Audit scope
CN=OISTE Server Root RSA G1, O=OISTE Foundation, C=CH	9AE36232A5189FFDDB353DFD26520C0[illegible]A651E6	[illegible]

Subordinate CA Information

Subject Name	Fingerprint	Allowed usage
CN=WISeKey CertifyID Server RSA CA 1, O=WISeKey, C=CH	AE70FF8A3E11C7F95C3BAB3C8FB55EF[illegible]6DDE4E	[illegible]

Appendix C: OID Inventory

OWGTM defines the following OID Schema to identify the different Certificate Profiles issued under the whole PKI.

These OID can be substituted or complemented by equivalent OID published by the CAB/Forum:

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 TLS 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 TLS Certificate - 7.4.7 – CertifyID Advanced OV TLS Certificate

- 7.4.8 – CertifyID Advanced EV TLS 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

Appendix D: Certificate Profiles

This section describes the certificate profiles issued by our CA, including all mandatory and optional extensions, based on the CAB Forum Baseline Requirements for TLS and S/MIME certificates and the EV Guidelines.

These following certificate profiles are illustrative of our certification practices. OWGTM ensures that the effective profiles are always aligned to the latest version of what stipulated in section 7 of this document and the applicable baseline requirements, in force at the moment of issuance.

Note: In all cases, serial numbers in new certificates contain at least 64 bits of output from a CSPRNG.

Infrastructure Certificates

Issuing CA Certificates

Note: Currently, OWGTM is only maintaining active unconstrained subordinate CA Certificates. This section would be updated before issuing new constrained or cross-signed CA Certificates.

Attribute	Content	Example Value	Notes
Version	v3	v3	**Mandatory**
Serial Number	Unique value assigned by Root CA	33:00:00:...	**Mandatory**
Signature Algorithm	sha256/384/512WithRSAEncryption with-SHA256/384/512	sha256WithRSAEncryption	**Mandatory**
Issuer	Root CA Subject Name	C=CH, O=WISeKey, OU=OISTE Foundation Endorsed, CN=OISTE WISeKey Global Root GB CA	**Mandatory**
Validity Period	Determined by Root CA; typically 10–25 years	2020-07-04 → 2035-07-04	**Mandatory**
Subject	Issuing CA identity	C=CH, O=WISeKey, CN=WISeKey CertifyID SSL GB CA 2	**Mandatory**
Public Key Algorithm / Size	RSA 2048/3072/4096 or EC P-256/P-384/P-521	RSA 2048	**Mandatory**
Basic Constraints (critical)	CA:TRUE, pathlen:0	CA:TRUE, pathlen:0	**Mandatory**; ensures this is a subordinated CA capable of issuing end-entity certificates
Key Usage (critical)	Certificate Sign, CRL Sign, Digital Signature (Optional)	Certificate Sign, CRL Sign	**Mandatory**; issuing CAs must not have Digital Signature or Key Encipherment
Extended Key Usage (EKU)	For TLS CAs: TLS Server Auth, TLS Client Auth (Optional)For S/MIME CAs: email Protection, TLS Client Auth (Optional)	TLS Web Server Authentication, TLS Web Client Authentication	**Mandatory** (per CABF BR)

Attribute	Content	Example Value	Notes
Subject Key Identifier (SKI)	keyid:...	keyid:5F:1B:C5:...	**Mandatory**
Authority Key Identifier (AKI)	keyid:...	keyid:35:0F:C8:...	**Mandatory**
CRL Distribution Points (CRL DP)	URI:...	http://public.wisekey.com/crl/ca	**Mandatory**
Authority Info Access (AIA)	CA Issuers URI, OCSP URI (Optional)	CA Issuers: http://public.wisekey.com/rca.crtOCSP:http://ocsp.wisekey.com/	**Mandatory**
Certificate Policies	Policy OID + CPS URI (Optional)	Policy: anyPolicyCPS: http://www.wisekey.com/repo/	**Mandatory**; Policy OIDs as mandated by the CABF BR
SAN	Not required for CA certificates	*Not present*	**Optional**
SCT List	Embedded SCTs	*Not present*	Not required for SubCAs

OCSP Responder Certificates

Attribute	Content	Example Value	Notes
Version	v3	v3	**Mandatory**
Serial Number	Unique value assigned by issuing CA	35:16:6B:...	**Mandatory**
Signature Algorithm	sha256/384WithRSAEncryption with-SHA256/384/512	sha256WithRSAEncryption	**Mandatory**
Issuer	Issuing CA Subject Name	C=CH, O=WISeKey, CN=WISeKey CertifyID SSL GB CA 2	**Mandatory**
Validity Period	Determined by CA; may be up to 1 year	2025-05-29 → 2026-05-29	**Mandatory**; OCSP responder certs typically short-lived
Subject	OCSP responder identity	C=CH, O=WISeKey, CN=WISeKey CertifyID SSL GB CA 2 OCSP	**Mandatory**
Public Key Algorithm / Size	RSA 2048/3072/4096 or EC P-256/P-384/P-521	RSA 2048	**Mandatory**
Basic Constraints (critical)	CA:FALSE	CA:FALSE	**Optional**
Key Usage (critical)	Digital Signature	Digital Signature	**Mandatory**; OCSP responder certificates **must not** allow key encipherment
Extended Key Usage (EKU)	OCSP Signing (id-kp-OCSPSigning)	OCSP Signing	**Mandatory**; must contain only id-kp-OCSPSigning
OCSP No Check	Present (non-critical)	OCSP No Check	**Optional** but recommended for responder certs
Subject Key Identifier (SKI)	keyid:...	keyID:5F:DE:F0:...	**Optional**
Authority Key Identifier (AKI)	keyid:....	keyid:5F:...	**Mandatory**
Authority Info Access (AIA)	OCSP & CA Issuers (optional for OCSP responder certs)	*Not present*	**Optional**

Attribute	Content	Example Value	Notes
CRL Distribution Points	URI:...	*Not present*	**Optional**
Certificate Policies	Policy OIDs (optional)	*Not present*	**Optional**
SCT list	Embedded SCTs	*Not present*	Not required for OCSP responder certs

TLS Certificate Profiles

TLS Certificates Validity Period Schedule

Certificate Type	Maximum Validity (Not After – Not Before)
DV / OV / EV	Until 15 Mar 2026: **398 days**
DV / OV / EV	15 Mar 2026 – 14 Mar 2027: **200 days**
DV / OV / EV	15 Mar 2027 – 14 Mar 2029: **100 days**
DV / OV / EV	From 15 Mar 2029: **47 days**

DV TLS Certificate Profile

Attribute	Content	Example Value	Notes
Version	v3	v3	**Mandatory**
Serial Number	Unique value	01:A3:4F...	**Mandatory**
Signature Algorithm	sha256/384WithRSAEncryption with-SHA256/384/512	sha256WithRSAEncryption	**Mandatory**
Issuer	<Issuer Subject Name>	C=CH, O=WISeKey, CN=GB DV CA	**Mandatory**
Validity Period	<See Schedule above>	2025-11-01 → 2025-11-22	**Mandatory**; capped per BR schedule
Subject	CN=<domain>	CN=gbdvvalidssl.hightrusted.com	**Optional**; SAN must be critical if not included
Public Key Algorithm / Size	RSA 2048/3072/4096EC P-256/P-384	RSA 2048	**Mandatory**
Basic Constraints (critical)	CA:FALSE	CA:FALSE	**Optional**
Key Usage (critical)	Digital Signature, Key Encipherment (as allowed for ECC certificates)	Digital Signature, Key Encipherment	**Mandatory**
Extended Key Usage	TLS Web Server Auth, TLS Web Client Auth (optional)	TLS Web Server Auth	**Mandatory**
SAN	DNS:<domain>	DNS:gbdvvalidssl.hightrusted.com	**Mandatory**; at least one
Certificate Policies	CABF OID + CPS URL (Optional) + Custom OID (Optional)	2.23.140.1.2.1, CPS: http://hightrusted.com/cps	**Mandatory**
Authority Key Identifier (AKI)	keyid:...	keyid:AB:CD:EF:12:34:56	**Mandatory**
Subject Key Identifier (SKI)	keyid:...	keyid:12:34:56:78:9A:BC	**Optional**

Attribute	Content	Example Value	Notes
Authority Info Access (AIA)	CA Issuers URI,OCSP URI (Optional)	CA Issuers: http://hightrusted.com/ca.crt, OCSP: http://ocsp.hightrusted.com	**Mandatory**
CRL Distribution Points (CRL DP)	URI:…	http://gbdvvalidssl.hightrusted.com/crl.pem	**Mandatory**
SCT list	present	Embedded SCTs	**Optional (but included)**

OV TLS Certificate Profile

Attribute	Content	Example Value	Notes
Version	v3	v3	**Mandatory**
Serial Number	Unique value	01:A3:4F…	**Mandatory**
Signature Algorithm	sha256/384WithRSAEncryption with-SHA256/384/512	sha256WithRSAEncryption	**Mandatory**
Issuer	<Issuer Subject Name>	C=CH, O=WISeKey, CN=GB DV CA	**Mandatory**
Validity Period	<See Schedule above>	2025-11-01 → 2025-11-22	**Mandatory**; capped per BR schedule
Subject	C, ST, O, CN=<domain> (or other combinations and fields allowed by the BR)	C=CH, ST=Zurich, O=Company, CN=gbovvalidssl.hightrusted.com	**Mandatory**
Public Key Algorithm / Size	RSA 2048/3072/4096EC P-256/P-384/P-521	RSA 2048	**Mandatory**
Basic Constraints (critical)	CA:FALSE	CA:FALSE	**Optional**
Key Usage (critical)	Digital Signature, Key Encipherment (as allowed for ECC certificates)	Digital Signature, Key Encipherment	**Mandatory**
Extended Key Usage	TLS Web Server Auth, TLS Web Client Auth (optional)	TLS Web Server Auth	**Mandatory**
SAN	DNS:<domain>	DNS:gbdvvalidssl.hightrusted.com	**Mandatory**; at least one
Certificate Policies	CABF OID + CPS URL (Optional) + Custom OID (Optional)	2.23.140.1.2.2, CPS: http://hightrusted.com/cps	**Mandatory**
Authority Key Identifier (AKI)	keyid:…	keyid:AB:CD:EF:12:34:56	**Mandatory**
Subject Key Identifier (SKI)	keyid:…	keyid:12:34:56:78:9A:BC	**Optional**
Authority Info Access (AIA)	CA Issuers URI,OCSP URI (Optional)	CA Issuers: http://hightrusted.com/ca.crt, OCSP: http://ocsp.hightrusted.com	**Mandatory**
CRL Distribution Points (CRL DP)	URI:…	http://gbdvvalidssl.hightrusted.com/crl.pem	**Mandatory**
SCT list	present	Embedded SCTs	**Optional (but included)**

EV TLS Certificate Profile

Attribute	Content	Example Value	Notes
Version	v3	v3	**Mandatory**
Serial Number	Unique value	01:A3:4F…	**Mandatory**
Signature Algorithm	sha256/384WithRSAEncryption with-SHA256/384/512	sha256WithRSAEncryption	**Mandatory**
Issuer	<Issuer Subject Name>	C=CH, O=WISeKey, CN=GB DV CA	**Mandatory**
Validity Period	<See Schedule above>	2025-11-01 → 2025-11-22	**Mandatory**; capped per BR schedule
Subject	C, ST, L, O, serialNumber, CN, businessCategory, jurisdictionStateOrProvinceName, jurisdictionCountryName (or other combinations and fields allowed by the BR and EVGL)	C=CH, ST=Zurich, O=Company, serialNumber=123456789, CN=gbevvalidssl.hightrusted.com, businessCategory=Private Organization, jurisdictionStateOrProvinceName=Zurich, jurisdictionCountryName=CH	**Mandatory**
Public Key Algorithm / Size	RSA 2048/3072/4096EC P-256/P-384/P-521	RSA 2048	**Mandatory**
Basic Constraints (critical)	CA:FALSE	CA:FALSE	**Optional**
Key Usage (critical)	Digital Signature, Key Encipherment (as allowed for ECC certificates)	Digital Signature, Key Encipherment	**Mandatory**
Extended Key Usage	TLS Web Server Auth, TLS Web Client Auth (optional)	TLS Web Server Auth	**Mandatory**
SAN	DNS:<domain>	DNS:gbdvvalidssl.hightrusted.com	**Mandatory**; at least one
Certificate Policies	CABF OID + CPS URL (Optional) + Custom OID (Optional)	2.23.140.1.1, CPS: http://hightrusted.com/cps	**Mandatory**
Authority Key Identifier (AKI)	keyid:…	keyid:AB:CD:EF:12:34:56	**Mandatory**
Subject Key Identifier (SKI)	keyid:…	keyid:12:34:56:78:9A:BC	**Optional**
Authority Info Access (AIA)	CA Issuers URI,OCSP URI (Optional)	CA Issuers: http://hightrusted.com/ca.crt, OCSP: http://ocsp.hightrusted.com	**Mandatory**
CRL Distribution Points (CRL DP)	URI:…	http://gbdvvalidssl.hightrusted.com/crl.pem	**Mandatory**
SCT list	present	Embedded SCTs	**Optional (but included)**

S/MIME Certificate Profiles

When including the usage for email protection, the commercial names of Personal Certificates will match the different classes defined by the CAB/Forum for S/MIME Certificates as indicated in this table:

Commercial names	CAB/F Designation
Standard CertificateBasic Certificate	mailbox-validated
Advanced Personal CertificateAdvanced Qualified Certificate	individual-validated
Advanced Professional CertificateQualified Professional Certificate	sponsor-validated
Advanced Corporate CertificateQualified Corporate Certificate	organization-validated

Currently, the S/MIME certificates issued by OWGTM will match the "multipurpose" profiles defined by the CAB/Forum.

S/MIME Certificates Validity Period Schedule

Certificate Type	Maximum Validity
Mailbox-validated	825 days
Individual-validated	825 days
Sponsor-validated	825 days
Organization-validated	825 days

Mailbox-Validated Certificate Profile

Attribute	Content	Example Value	Notes
Version	v3	v3	**Mandatory**
Serial Number	Unique value	14:b4:...	**Mandatory**
Signature Algorithm	sha256/384WithRSAEncryption with-SHA256/384/512	sha256WithRSAEncryption	**Mandatory**
Issuer	<Issuer Subject Name>	C=CH, O=WISeKey, CN=WISeKey CertifyID CA X	**Mandatory**
Validity Period	<See Schedule above>	Not Before: Oct 30 2025 16:10:52 GMT Not After: Oct 30 2027 16:10:51 GMT	**Mandatory**; Max 825 days in current CAB Forum S/MIME requirements
Subject	CN, emailAddress (or other combinations and fields allowed by the SMIME BR)	CN=john.smith@example.com, emailAddress=john.smith@example.com	**Mandatory**
Public Key Algorithm / Size	RSA 2048/3072/4096P-256/P-384/P-521	RSA 2048	**Mandatory**
Basic Constraints (critical)	CA:FALSE	CA:FALSE	**Optional**
Key Usage (critical)	A valid combination of Digital Signature, nonRepudiation, Data Encipherment, Key Encipherment and/or Key Agreement	Digital Signature	**Mandatory**
Extended Key Usage	E-mail Protection (Mandatory)TLS Web Client Auth and other allowed fields (Optional)	E-mail Protection	**Mandatory**

Attribute	Content	Example Value	Notes
Subject Alternative Name (SAN)	email:	email:john.smith@example.com	**Mandatory** (at least one)
Certificate Policies	CABF OID (Mandatory), CPS URI and other OID as allowed by the SMIME BR (Optional)	CABF OID	**Mandatory**
Authority Key Identifier (AKI)	keyID:...	keyid:DB:68:...	**Mandatory**
Subject Key Identifier (SKI)	keyID:...	keyID:0C:D1...	**Optional**
Authority Info Access (AIA)	CA Issuers URI,OCSP URI (Optional)	CA Issuers: http://hightrusted.com/ca.crt, OCSP: http://ocsp.hightrusted.com	**Mandatory**
CRL Distribution Points (CRL DP)	URI:...	URI: http://public.wisekey.com/ca.crl	**Mandatory**

Individual-Validated Certificate Profile

Attribute	Content	Example Value	Notes
Version	v3	v3	**Mandatory**
Serial Number	Unique value	14:b4:...	**Mandatory**
Signature Algorithm	sha256/384WithRSAEncryption with-SHA256/384/512	sha256WithRSAEncryption	**Mandatory**
Issuer	<Issuer Subject Name>	C=CH, O=WISeKey, CN=WISeKey CertifyID CA X	**Mandatory**
Validity Period	<See Schedule above>	Not Before: Oct 30 2025 16:10:52 GMT Not After: Oct 30 2027 16:10:51 GMT	**Mandatory**; Max 825 days in current CAB Forum S/MIME requirements
Subject	C, ST, L, SN, GN, CN, emailAddress (or other combinations and fields allowed by the SMIME BR)	C=CH, L=Geneve, SN=Smith, GN=John, CN=john.smith@example.com, emailAddress=john.smith@example.com	**Mandatory**
Public Key Algorithm / Size	RSA 2048/3072/4096P-256/P-384/P-521	RSA 2048	**Mandatory**
Basic Constraints (critical)	CA:FALSE	CA:FALSE	**Optional**
Key Usage (critical)	A valid combination of Digital Signature, nonRepudiation, Data Encipherment, Key Encipherment and/or Key Agreement	Digital Signature	**Mandatory**
Extended Key Usage	E-mail Protection (Mandatory)TLS Web Client Auth and other allowed fields (Optional)	E-mail Protection	**Mandatory**
Subject Alternative Name (SAN)	email:	email:john.smith@example.com	**Mandatory** (at least one)

Attribute	Content	Example Value	Notes
Certificate Policies	CABF OID (Mandatory), CPS URI and other OID as allowed by the SMIME BR (Optional)	CABF OID	**Mandatory**
Authority Key Identifier (AKI)	keyID:...	keyid:DB:68:...	**Mandatory**
Subject Key Identifier (SKI)	keyID:...	keyID:0C:D1...	**Optional**
Authority Info Access (AIA)	CA Issuers URI,OCSP URI (Optional)	CA Issuers: http://hightrusted.com/ca.crt, OCSP: http://ocsp.hightrusted.com	**Mandatory**
CRL Distribution Points (CRL DP)	URI:...	URI: http://public.wisekey.com/ca.crl	**Mandatory**

Sponsor-Validated Certificate Profile

Attribute	Content	Example Value	Notes
Version	v3	v3	**Mandatory**
Serial Number	Unique value	14:b4:...	**Mandatory**
Signature Algorithm	sha256/384WithRSAEncryption with-SHA256/384/512	sha256WithRSAEncryption	**Mandatory**
Issuer	<Issuer Subject Name>	C=CH, O=WISeKey, CN=WISeKey CertifyID CA X	**Mandatory**
Validity Period	<See Schedule above>	Not Before: Oct 30 2025 16:10:52 GMT Not After: Oct 30 2027 16:10:51 GMT	**Mandatory**; Max 825 days in current CAB Forum S/MIME requirements
Subject	C, ST, L, OU, O, organizationIdentifier, SN, GN, CN, emailAddress (or other combinations and fields allowed by the SMIME BR)	C=CH, ST=Geneve, O=WISeKey SA, organizationIdentifier=NTRCH-CHE-101.022.134, SN=Smith, GN=John, CN=john.smith@example.com, emailAddress=john.smith@example.com	**Mandatory**
Public Key Algorithm / Size	RSA 2048/3072/4096P-256/P-384/P-521	RSA 2048	**Mandatory**
Basic Constraints (critical)	CA:FALSE	CA:FALSE	**Optional**
Key Usage (critical)	A valid combination of Digital Signature, nonRepudiation, Data Encipherment, Key Encipherment and/or Key Agreement	Digital Signature	**Mandatory**
Extended Key Usage	E-mail Protection (Mandatory)TLS Web Client Auth and other allowed fields (Optional)	E-mail Protection	**Mandatory**
Subject Alternative Name (SAN)	email:	email:john.smith@example.com	**Mandatory** (at least one)

Attribute	Content	Example Value	Notes
Certificate Policies	CABF OID (Mandatory), CPS URI and other OID as allowed by the SMIME BR (Optional)	CABF OID	**Mandatory**
Authority Key Identifier (AKI)	keyID:...	keyid:DB:68:...	**Mandatory**
Subject Key Identifier (SKI)	keyID:...	keyID:0C:D1...	**Optional**
Authority Info Access (AIA)	CA Issuers URI,OCSP URI (Optional)	CA Issuers: http://hightrusted.com/ca.crt, OCSP: http://ocsp.hightrusted.com	**Mandatory**
CRL Distribution Points (CRL DP)	URI:...	URI: http://public.wisekey.com/ca.crl	**Mandatory**

Organization-Validated Certificate Profile

Attribute	Content	Example Value	Notes
Version	v3	v3	**Mandatory**
Serial Number	Unique value	14:b4:...	**Mandatory**
Signature Algorithm	sha256/384WithRSAEncryption with-SHA256/384/512	sha256WithRSAEncryption	**Mandatory**
Issuer	<Issuer Subject Name>	C=CH, O=WISeKey, CN=WISeKey CertifyID CA X	**Mandatory**
Validity Period	<See Schedule above>	Not Before: Oct 30 2025 16:10:52 GMT Not After: Oct 30 2027 16:10:51 GMT	**Mandatory**; Max 825 days in current CAB Forum S/MIME requirements
Subject	C, ST, L, OU, O, organizationIdentifier, CN, emailAddress (or other combinations and fields allowed by the SMIME BR)	C=CH, ST=Geneve, O=WISeKey SA, organizationIdentifier=NTRCH-CHE-101.022.134, CN=WISeKey SA, emailAddress=john.smith@example.com	**Mandatory**
Public Key Algorithm / Size	RSA 2048/3072/4096P-256/P-384/P-521	RSA 2048	**Mandatory**
Basic Constraints (critical)	CA:FALSE	CA:FALSE	**Optional**
Key Usage (critical)	A valid combination of Digital Signature, nonRepudiation, Data Encipherment, Key Encipherment and/or Key Agreement	Digital Signature	**Mandatory**
Extended Key Usage	E-mail Protection (Mandatory)TLS Web Client Auth and other allowed fields (Optional)	E-mail Protection	**Mandatory**
Subject Alternative Name (SAN)	email:	email:john.smith@example.com	**Mandatory** (at least one)

Attribute	Content	Example Value	Notes
Certificate Policies	CABF OID (Mandatory), CPS URI and other OID as allowed by the SMIME BR (Optional)	CABF OID	**Mandatory**
Authority Key Identifier (AKI)	keyID:...	keyid:DB:68:...	**Optional**
Subject Key Identifier (SKI)	keyID:...	keyID:0C:D1...	**Optional**
Authority Info Access (AIA)	CA Issuers URI,OCSP URI (Optional)	CA Issuers: http://hightrusted.com/ca.crt, OCSP: http://ocsp.hightrusted.com	**Mandatory**
CRL Distribution Points (CRL DP)	URI:...	URI: http://public.wisekey.com/ca.crl	**Mandatory**

Non-S/MIME Personal/Device Certificate Profiles

OWGTM allows the issuance of "Personal" or "Device" certificates that don't include the EKUs for TLS Server Authentication or Email Protection (S/MIME). These certificates will be typically intended for: - **Client Authentication**: Certificates issued by "Non-TLS" Certification Authorities that are mainly used for TLS Client Authentication. - **Document Signature**: Certificates issued by "Non-TLS" Certification Authorities that are used for digital signature of documents (i.e. Adobe PDF documents).

These certificates will use generally profiles consistent with the examples above for S/MIME certificates, without including the EKU for email protection.

When issued by publicly-trusted Issuing CAs covered by this CPS, these certificates will be subject to the rules derived of the compliance requirements for the particular Root under which are issued.

Appendix E: Version history

Combined CP/CPS document (this document)

VERSION	DATE	MODIFICATION	AUTHOR
4.0	9/12/2024	First consolidated CP/CPS	Pedro Fuentes
4.0.1	13/1/2025	Minor changes	Pedro Fuentes
4.0.2	21/3/2025	Minor changes	Pedro Fuentes
4.0.3	27/6/2025	Minor changes	Pedro Fuentes
4.0.4	DRAFT	Statement for Mass Revocation	Pedro Fuentes
4.1	26/11/2025	Wording improvements to address root program feedback	Pedro Fuentes

Previous versions

Previously to combining the CP and CPS in a single document (this document), the OISTE/WISeKey Trust Model published separate CP documents for each type of certificate and separate CPS documents for OISTE (covering the Root CAs) and WISeKey (covering the subordinate CAs). The previous documents and their version history are available at https://oiste.org/repository and https://wisekey.com/repository, respectively.