OISTE-WISeKey Global Trust Model

Certification Practices Statement (CPS)

Date: 02/06/2015	**Version**: 2.2
Status: FINAL	**No. of Pages**: 77
OID: 2.16.756.5.14.7.1	**Classification**: PUBLIC
File: WKPKI.DE001 - OWGTM PKI CPS.v2.2b-CLEAN.docx	
Published by: WISeKey SA – Policy Approval Authority	

Documentation management

Document Approval

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

Version history

Version	Date	Comments
1.0	1/12/2005	First version
1.01	16/1/2007	Modification on section 2.8.1.2 stating that "WISeKey hereby grants a non-exclusive and irrevocable license to all Certification Authorities, Relying Parties and other entities to reproduce, and distribute copies of the certificates issued within the OISTE WISeKey Root PKI for the purposes of providing, using and/or relying on the certificates and certification services in accordance with the provisions of this CPS."
1.02	5/3/2012	Modification on section 2.1.2 to add an obligation for Policy CAs to control and avoid the issuance of certificates to subordinated Certification Authorities that don't check the ownership of the domain included in the end user certificates.
1.1	1/12/2014	Modification on section 1.3.1 to add the new Generation B Root CA
2.0	1/5/2015	Major change to adopt RFC3647 and CABF compliance
2.1	29/5/2015	Minor changes to complete OID list for GA hierarchy and complete certificate details for the GB Policy CA
2.2	2/6/2015	Minor changes to address audit requirements

Contents

1 Introductions

1.1 Overview

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

The OISTE-WISeKey Global Trust Model (**OWGTM**) have 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) and is intended to serve as a common services infrastructure for Certification Authorities worldwide that comply with WISeKey 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 the International Organization for Secure Electronic Transactions ("IOSET" or "OISTE"), a Swiss non-profit foundation established in 1998, and recognized with an "Special Consultative Status" by the United Nations. The OISTE Foundation maintains a Policy Approval Authority (OFPAA or PAA) that drafts, approves and revises the policies to which WISeKey is bound to comply with under its operator contract. The OFPAA is composed of members of the community to which OISTE provides its Certification Authority Services, resulting in a virtuous cycle for trust management.

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 according to the recommendations found in the document **RFC3647** issued by *The Internet Society* in 2003, 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.
3. Identification and Authentication – Discloses the rules for subscriber naming and required authentication policies.
4. Certificate Life-Cycle Operational Requirements – This section describes the different phases in the Life-Cycle of certificates and their requirements.
5. Management, Operational and Physical Controls – Describes the controls enforced in the **OWGTM** to provide adequate trust levels in the certificates issued under the Trust Model.
6. Technical Security Controls – Discloses the security controls adopted in the **OWGTM**.
7. Certificate and CRL Profiles – Describes the technical details of the different certificate types issued under the **OWGTM**.
8. Compliance Audit and other Assessment – Discloses the audit policies followed in the **OWGTM** to ensure that the participant fulfils the security and quality requirements.
9. Other Business and Legal Matters – This section exposes the commercial, legal and contractual aspects involved in the usage of certificates issued in the **OWGTM**.

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

- The Certification Practices Statement (CPS) –The CPS is a statement of the practices that every Certification Authority operating under the **OWGTM** Trust Model employs in issuing, managing, revoking, and renewing or re-keying certificates.
- A number of Certificate Policies (CP) – each being a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. The currently approved CPs are incorporated in this version of the CPS, as summarized in Annex B: Approved Certificate Policies and Profiles. ***Any explicit mention to a CP document must be understood as referring to this document; OWGTM does not maintain separate CP documents***.

The CPS and CP information follow the same structure and are integrated in this document, being the single reference for all the certification practices and policies managed under the **OWGTM**.

1.2 Document Name and Identification

Name	OWGTM Certification Practices Statement
Version	2.0
OID	2.16.756.5.14.7.1
Issuance date	1st of May, 2015
Location	This document can be found at http://www.wisekey.com/repository

1.3 PKI Participants

1.3.1 Certification authorities

The following diagram is a graphical representation **OWGTM** CA Hierarchy.

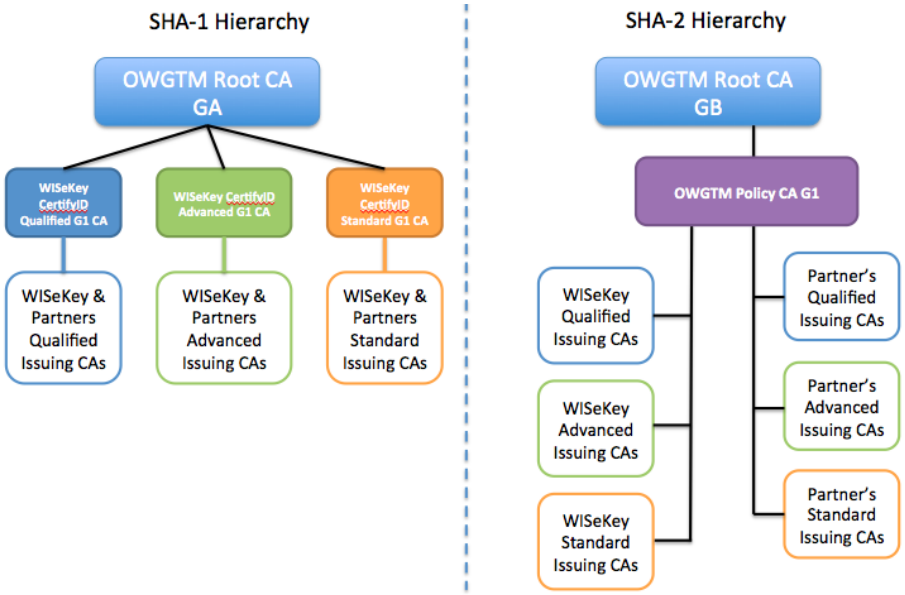

Figure: Certification Authorities' hierarchy

At the moment of writing this document, both hierarchies are considered as equally active, although the branches below the SHA-1 algorithms are in the process of being deprecated, in favour of the SHA-2 hierarchy, which should become the only one active at a given moment.

The Certification Authorities that compose the **OWGTM** are disclosed in the following sub-section.

1.3.1.1 Root Certification Authorities

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

Short name	OWGTM Root CA GA
Distinguished Name	CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH
SHA-1 Fingerprint	59 22 A1 E1 5A EA 16 35 21 F8 98 39 6A 46 46 B0 44 1B 0F A9
Issued by	<SELF-SIGNED>
Issuance date	11 of December, 2005
Expiration date	11 of December, 2037
Location	This certificate, in the common standard formats, can be found in http://www.wisekey.com/repository

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

1.3.1.2 Intermediary Certification Authorities

- "**OWGTM Policy CA G1**" is a Certification Authority subordinated to the "OWGTM Root CA GB". This CA issue certificates for "Issuing CAs" (Certification Authorities that issue certificates for End Entities) dedicated to specific entities and/or purposes, but this CA itself does not issue certificates to end entities. The identification data of the "**OWGTM Policy CA G1**" is included in the following table:

Short name	OWGTM POLICY CA GB 1
Distinguished Name	CN=WISeKey CertifyID Policy GB CA 1, O=WISeKey, C=CH
SHA-1 Fingerprint	63 8E F7 24 26 BD 7A 8F 61 A5 78 CD F3 C6 29 57 EE 03 8F 32
Issued by	OWGTM Root CA GB
Issuance date	13th of May, 2015
Expiration date	1st of September, 2039
Location	This certificate, in the common standard formats, can be found in http://www.wisekey.com/repository

- "**WISeKey CertifyID Qualified G1 CA**" is a subordinated Certification Authority of the "**OWGTM Root CA GA**". This CA is responsible for issuing certificates of "Issuing CAs" associated to the "QUALIFIED CERTIFICATE CLASS", but this CA itself does not issue certificates to end entities. This intermediary CA is in the process of being deprecated until the SHA-2 algorithm is fully adopted. The identification data of this CA is included in the following table:

Distinguished Name	CN=WISeKey CertifyID Qualified G1 CA, OU=International, OU= Copyright (c) 2006 WISeKey SA , O=WISeKey, C=CH
SHA-1 Fingerprint	BD 59 C8 B9 E2 76 CC 0E EC EF 03 26 3B A6 63 C1 7D AE FA 98
Issued by	OWGTM Root CA GA
Issuance date	17th of October, 2006
Expiration date	17th of October, 2021
Location	This certificate, in the common standard formats, can be found in http://www.wisekey.com/repository

- "**WISeKey CertifyID Advanced G1 CA**" is a subordinated Certification Authority of the "**OWGTM Root CA GA**". This CA is responsible for issuing certificates of "Issuing CAs" associated to the "ADVANCED CERTIFICATE CLASS", but this CA itself does not issue certificates to end entities. This intermediary CA is in the process of being deprecated until the SHA-2 algorithm is fully adopted. The identification data of this CA is included in the following table:

Distinguished Name	CN=WISeKey CertifyID Advanced G1 CA, OU=International, OU= Copyright (c) 2005 WISeKey SA , O=WISeKey, C=CH
SHA-1 Fingerprint	9C EF ED B3 3C 24 8D 16 FC CF D0 8C 62 CD 44 BC 56 A0 D5 F0
Issued by	OWGTM Root CA GA
Issuance date	11th of December, 2011
Expiration date	11th of December, 2020
Location	This certificate, in the common standard formats, can be found in http://www.wisekey.com/repository

- "**WISeKey CertifyID Standard G1 CA**" is a subordinated Certification Authority of the "**OWGTM Root CA GA**". This CA is responsible for issuing certificates of "Issuing CAs" associated to the "STANDARD CERTIFICATE CLASS", but this CA itself does not issue certificates to end entities. This intermediary CA is in the process of being deprecated until the SHA-2 algorithm is fully adopted. The identification data of this CA is included in the following table:

Distinguished Name	CN=WISeKey CertifyID Standard G1 CA, OU=International, OU= Copyright (c) 2005 WISeKey SA , O=WISeKey, C=CH
SHA-1 Fingerprint	9D 72 1A 47 CB CA CD D7 FE 10 DE A0 6C EB 3C 99 21 6D 46 15
Issued by	OWGTM Root CA GA
Issuance date	23th of December, 2005
Expiration date	23th of December, 2020
Location	This certificate, in the common standard formats, can be found in http://www.wisekey.com/repository

1.3.1.3 Issuing Certification Authorities

OWGTM Issuing Certification Authorities. End Entity certificates are issued by a particular "Issuing CA" that was generated under "OWGTM Root CA GB" or a particular "Policy CA", depending on the characteristics of that Entity. These Issuing CAs will be accredited to issue a certain type (or types) of certificates, each conforming to a "Certificate Policy" (CP) or "Class" ("Standard", "Advanced" or "Qualified"), as indicated in Annex B: Approved Certificate Policies and Profiles. A list of accredited Issuing CAs can be found at http://www.wisekey.com/repository.

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

1.3.2 Registration authorities

The Registration Authorities 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 CP.

The Registration Authorities in the **OWGTM** are directly controlled by the owner of an "Issuing CA" and follow an accreditation process imposed by the **OWGTM** in order to ensure that all security and operational procedures related to the certificates life-cycle are strictly enforced. Therefore, within the **OWGTM** environment there exists locations titled "**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:

[1] WISeKey itself is not considered an affiliate, be being a main component of **OWGTM**.

- 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.

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.

In the **OWGTM** Trust Model, the Certificate Policy (CP) 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 persons and entities that trust the certificates issued by certification authorities operating under the **OWGTM** Trust Model are considered to be "relying parties" (or trusted third parties). These relying parties do not necessarily need to be a subscriber of an **OWGTM** certificate, but are requested to accept the "**OWGTM** Relying Party agreement".

In the **OWGTM** Trust Model, a particular Certification Policy could limit the right to be a relying party for a particular type of certificate.

1.3.5 Other participants

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

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

OWGTM reserves the right to delegate these services to third parties. These participants will follow an accreditation process defined by the **OWGTM**.

1.4 Certificate Usage

In the **OWGTM**, the limitations for certificate usage are established by the Certificate Policy corresponding to each particular certificate type, according to the following subsections.

1.4.1 Appropriate certificate uses

1.4.1.1 Personal Certificates

CP Identifier	Description	Permitted uses
CertifyID Standard Personal Certificate	Low assurance personal certificate, primarily used for authentication and e-mail security. Only the e-mail is verified.	Digital Signature, Encryption, Client Authentication
CertifyID Advanced Personal Certificate	Medium/High[2] assurance personal certificate. Recommended for legally binding digital signatures in corporate environments. All identification attributes in the certificate are verified. Remote verification is allowed under certain circumstances.	Digital Signature, Encryption, Client Authentication, Non-Repudiation
CertifyID Qualified Personal Certificate	High assurance certificate. Recommended for legally binding signatures on open environments. All identification attributes in the certificate are verified "Face-to-Face".	Digital Signature, Encryption, Client Authentication, Non-Repudiation

1.4.1.2 Corporate and Server Certificates

CP Identifier	Description	Permitted uses
CertifyID Standard SSL[3] Certificate	Medium assurance SSL/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, Client Authentication
CertifyID Advanced OV SSL Certificate	High assurance SSL/TLS certificate. All identification attributes in the	Digital Signature, Encryption, Client Authentication, Server

[2] This certificate is considered as "High assurance" when the private key is protected by a "secure signature device" (i.e. Smartcard or other hardware+software solution that ensures unique control con the key
[3] Note: SSL Certificates can be offered in different versions (e.g. Wildcard or Unified Communications), but always according to the applicable base CP and CA/Browser Forum requirements.

	certificate are verified. The Identity of the organization is validated. Compliant with CA/Browser Forum Baseline Requirements.	Authentication
CertifyID Advanced EV SSL Certificate	High assurance SSL/TLS certificate. 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, Client Authentication, Server Authentication
CertifyID Qualified Corporate Certificate	High assurance certificate identifying a Juridical Person or Organization. Recommended for Digital Signatures issued in behalf of the organization and not by an individual person. All identification attributes in the certificate are verified "Face-to-Face".	Digital Signature, Encryption, Client Authentication, Non-Repudiation

1.4.1.3 Infrastructure Certificates

CP Identifier	Description	Permitted uses
Issuing CA Certificate	Subordinate Certification Authorities operating in the PKI will obtain a certificate as regulated by this CPS.	Certificate Signing
CertifyID URA Admin Certificate	Special User Certificate that allows access to the Universal Registration Authority platform. This certificate is issued to an individual acting as or in behalf of the Registration Authority and enforces the usage of strong authentication by only allowing the corresponding private key to be stored in a secure hardware device.	Digital Signature, Encryption, Client Authentication
CertifyID OCSP Certificate	Infrastructure certificate for Online Certificate Status Responders operating in the PKI. The certificate is defined as per the related RFC.	OCSP Response Signature
CertifyID TSA Certificate	Infrastructure certificate for Time Stamping Authorities operating in the PKI. The certificate is defined as per the related RFC and is regulated by the **OWGTM TSP** document.	Time Stamps Signature

1.4.2 Prohibited certificate uses

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

1.5 Policy Administration

1.5.1 Organization administering the document

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

The **OWGTM PAA** has a series of distinct functions but does not operate as a separate legal Entity. It is managed and organised in accordance with a process that draws on expertise within WISeKey and the OISTE Foundation. The **OWGTM 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 of the OISTE Foundation.

1.5.2 Contact Person (Contact Information)

Name	OWGTM Policy Approval Authority
email address	cps@wisekey.com
Address	29, route de Pré-Bois Case postale 885 CH-1215 Geneva 15 (Switzerland)

1.5.3 Person determining CPS suitability for the policy

The competent entity which determines the compliance and suitability of this 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).

1.6 Definitions and Acronyms

Definitions and Acronyms are included in Annex A: Glossary.

1.7 Statement Compliance with CA/Browser Forum requirements

WISeKey, as operator of the **OWGTM** ensures the compliance with industry best practices and security controls. In particular, **OWGTM** enforces compliance with the “Baseline Requirements” and “Extended Validation Requirements” for the certificate profiles to which these regulations apply.

2 Publication and Repository Responsibilities

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

2.1 Repositories

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

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

- Policies repository. This repository is a set of web pages and services available at the URL http://www.wisekey.com/repository
- Private Certificate repositories. The certificates are published for the subscriber of the certificate and registration authority members associated to the Issuing CA. The details of this access are appropriately communicated to the participants. Certificates published by Certification Authorities operated by WISeKey SA are accessible through the different software solutions made available by WISeKey to the participants.
- Public Certificate repositories. Publicly accessible certificate information repositories optionally maintained by the operators of the Certification Authorities operating under the **OWGTM** are disclosed appropriately to the relying parties of these certificates. Any Certificate Repository made available by WISeKey is listed in http://www.wisekey.com/repository.

2.2 Publication

The **OWGTM** is responsible for publication of information regarding practices, certificates, and the current status of certificates. Where appropriate, such responsibilities may be delegated to the "Issuing CAs" operating within the **OWGTM** Trust Model.

Issued certificates are published according to their specific Certificate Policy. These details are established as indicated in the previous version.

2.3 Time or frequency of publication

The CPS and CP documents will be published every time they are modified.

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 control on repositories

The access for reading information in the **OWGTM** ***public*** repositories is free and unlimited.

Only **OWGTM** Certifications and Registration Authorities are authorized to modify the information contained in its repositories. The **OWGTM** implements adequate controls to restrict the ability of modifying these repositories to authorized entities only.

3 Identification and Authentication

Certificates issued under the **OWGTM** follows a set of required minimum controls that ensure the authenticity of the data included in certificates. These controls are enforced during the full lifecycle of certificates, certificate requests, and related documents. If non-validated attributes are allowed for a certain type of certificate, it will be explicitly indicated in this document and/or in the certificate itself.

This document reflects the common policies and controls for Identification and Authentication. Controls which are specific to some types of certificate are stipulated explicitly in Annex C: Identity Validation Policies.

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

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity of subscribers and pseudonyms

Anonyms and pseudonyms are only supported in Distinguished Names of the "CertifyID Standard Personal Certificate" class.

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 ISO/IEC 9595 (X.500) Distinguished Name (DN) standard.

3.1.4.1 Issuing Certification Authorities

Common Name (CN)	[Unique identifier for the CA][4]
Organization Unit (OU)	(Optional) A set of optional values as complementary identity attributes, trademarks or copyright notices
Organization (O)	Publicly recognized name of the entity operating the Issuing CA
Locality (L)	(Optional) Locality where is based the operating entity
State (S)	(Optional) State or Province where is based the operating entity
Country (C)	Country where is based the operating entity

[4] The CN of the CA must include the identifier of the certificate class, as "Standard", "Advanced" or "Qualified"

3.1.4.2 End-Entity Subscriber Certificates

The current allowed names are specified as part of the different certificate profiles supported in the **OWGTM**. The current list is available in this document, at Annex B: Approved Certificate Policies and Profiles.

3.1.5 Uniqueness of names

The Distinguished Names in the **OWGTM** must be unique and never lead to ambiguity among the subscribers associated to a particular Issuing CA. This is ensured by a set of techniques and procedures implemented at various levels of the PKI, generally by the inclusion of a unique e-mail address per subscriber.

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 of a name.

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

3.2 Initial Identity Validation

"Initial Identity Validation" is the process of verifying the identity of an applicant and the authenticity of a certificate request. In general these aspects could depend on the certificate type, being specified, in such case, appropriately in Annex C: Identity Validation Policies.

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 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

This information is specified in Annex C: Identity Validation Policies.

3.2.3 Authentication of individual identity

This information is specified in Annex C: Identity Validation Policies.

3.2.4 Non-verified subscriber information

In general, any identity information included in the "Common Name" component in "CertifyID Standard Personal Certificate".

Other non-verified subscriber information, if any, will be made relevant as a notice in an "OU" component of the certificate.

3.2.5 Validation of authority

This information is specified in Annex C: Identity Validation Policies.

3.2.6 Criteria for interoperation

A Certification Authority that wishes to interoperate with the **OWGTM** is required to undergo an 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 Policies.

3.3 Identification and Authentication for Re-key Requests

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

3.3.1 Identification and authentication for routine re-key

For Issuing CAs, **OWGTM** doesn't support automated re-key or renewals. The applying entity must follow a formal CA Key Creation Ceremony and a designated officer will appropriately verify that the information included in the CA certificate are valid.

For end-entity certificates managed using a RA interface implemented or provided by WISeKey SA, the subscriber or an authorized Registration Officer can use his access credentials to initiate and approve, respectively, a certificate re-key or renewal. For classes other than the "CertifyID Standard Personal", the registration officer must validate that the identity attributes to be included in the new certificate are still valid before approving the request.

OWGTM Partners not using the RA interface provided by WISeKey, must implement the appropriate security controls to ensure that the security levels aren't affected. These controls must be disclosed and accepted by the **OWGTM** before the partner starts its operations.

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 procedures for its issuance.

3.4 Identification and Authentication for Revocation Requests

The Identification Policy for revocation requests is the same as stipulated for initial registration. Telematics requests will be only accepted if these include a digital signature using the subscriber certificate that is requested for revocation, or the certificate from a party that is authorized to request revocation on behalf of the subscriber.

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.

The **OWGTM** Certification and/or Registration Authorities can request the revocation of a certificate if there is knowledge or justified suspicion that the associated Private Key has been compromised, or reason to believe any other fact that recommends this action.

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.

4.1 Certificate Application

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.

4.1.1 Who can submit a certificate application

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

4.1.2 Enrolment process and responsibilities

The enrolment process, including the verified information and attributions to execute the process is detailed in the Annex C: Identity Validation Policies, (section 12 of this document).

In particular and where applicable, CAs will respect the requirements set by the CA/Browser Forum Baseline and EV Requirements.

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

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.

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 CPS and the appropriate Certificate Policy.

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

4.2.3 Time to process certificate applications

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

4.3 Certificate Issuance

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 than 39 months, according to the CA/Browser Forum 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 request received by a Registration Authority is genuine. The particular controls are stipulated in the appropriate Certificate Policy.

4.3.2 Notifications to subscriber by the CA of issuance of certificate

After a certificate is issued, the CA notifies the Registration Authority of the issuance and availability of the certificate, and the new certificate is published to the certificate repository.

The notification mechanism can be agreed specifically with the subscriber. In general, for personal certificates, the Registration Authority is responsible for notifying the subscriber of the availability of his certificate, by sending him a copy or by specifying how the certificate can be obtained.

Electronic notifications may be digitally signed by the Registration Authority or entitled representative.

4.4 Certificate Acceptance

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

4.4.1 Conduct constituting certificate acceptance

Certificate acceptance is understood after the subscriber or his representative performs one or more of the following:

- Signs 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 availability 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

As stated in section 4.3.2, 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.

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

The specific usages allowed for a private key associated to a certificate type issued in the **OWGTM** are as detailed in section 1.4.1 of this document.

4.5.2 Relying party public key and certificate usage

Relying parties must access and use the public key and certificate as stipulated in this CPS and as indicated in the "Relying Party Agreement" document, made public at the web page http://www.wisekey.com/repository.

4.6 Certificate Renewal

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

4.6.1 Circumstance for certificate renewal

A certificate can only be renewed for Personal and Corporate certificates, which are still valid and nearing expiration. The renewal of expired certificates is not supported by 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

The request of certificate renewals will be processed by the appropriate Registration Officer, verifying that none of the attributes of the new certificate have been changed in the last 39 months, as per the Baseline Requirements. Any change in an attribute will be conveniently validated, as defined in the relevant sections of this CPS.

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

As stipulated in section 4.4.2 of this document.

4.6.7 Notification of certificate issuance by the CA to other entities

As stated in section 4.3.2, 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.

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 still valid or already expired 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

The request of certificate re-key will be processed by the appropriate Registration Officer, verifying that none of the attributes of the new certificate have been changed in the last 39 months, as per the Baseline Requirements. Any change in an attribute will be conveniently validated, as defined in the relevant sections of this CPS.

4.7.4 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.

4.7.5 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

As stipulated in section 4.4.2 of this document.

4.7.7 Notification of certificate issuance by the CA entities

As stated in section 4.3.2, 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.

4.8 Certificate Modification

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

4.8.1 Circumstance for certificate modification

No stipulations.

4.8.2 Who may request certificate modification

No stipulations.

4.8.3 Processing certificate modification requests

No stipulations.

4.8.4 Notification of new certificate issuance to subscriber

No stipulations.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulations.

4.8.6 Publication of the modified certificate by the CA

No stipulations.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulations.

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 either revoking or suspending that certificate.

Suspension of certificates is only supported for personal certificates, and explicitly disallowed for SSL certificates, according to the CA/Browser Forum requirements.

4.9.1 Circumstances for revocation

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

1. The subscriber requests revocation of his/her certificate.
2. The subscriber indicates that the original certificate was not authorized and doesn't retroactively grant authorization.
3. The CA obtains reasonable evidence that the subscriber's private key (corresponding to the public key in the certificate) has been compromised or is suspected of compromise, or the certificate has otherwise been misused.
4. The CA receives notice or otherwise becomes aware that a subscriber has violated one or more of its material obligations under the subscriber agreement or terms of use.
5. The CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a subscriber's right to use a name (e.g. a domain name) listed in the certificate, or that the subscriber has failed to renew its right to use that name.
6. The CA receives notice or otherwise becomes aware of a material change in the information contained in the certificate.
7. A determination, in the CA's sole discretion, that the certificate was not issued in accordance of the terms and conditions derived for the appropriate Certificate Policy
8. The CA determines that any of the information appearing in the certificate is not accurate.
9. The CA ceases operations for any reason and has not arranged for another CA under the **OWGTM** to provide revocation support for the certificate.
10. The CA's right to issue certificates for a particular Certificate Policy expires or is revoked or terminated, unless the CA makes arrangements to continue maintaining the CRL/OCSP repository.
11. The private key of any CA in the certification path is suspected to have been compromised
12. The subscriber is a participant in the PKI (e.g. Registration Officer) and loses his right to access to keep acting as such.
13. The CA receives notice or otherwise becomes aware that a subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a place or in a manner that is prohibited under the laws and jurisdiction of the country of operation of the CA.

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

4.9.2 Who can request revocation

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

The authorized Registration Authority or entitled representative can request the revocation of a certificate if any of the circumstances expressed in the previous section is meet.

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.

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 under the OWGTM Trust Model.

Revocation requests communicated by other means (i.e. by non-signed electronic messages or by telephone) which do not unequivocally authenticate the requestor will produce a temporary suspension of the certificate, as defined in sections 4.9.13 to 4.9.16.

In particular, processing revocation for SSL 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 the Registration or Certification Authority.

4.9.5 Time within which CA must process the revocation request

Revocation requests are processed by the CA within the shortest possible period.

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 by using the **OWGTM Online Certificate Status Protocol Server** (referred as **OWGTM** 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 stipulated frequencies are:

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

- 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 every day, with a typical overlapping period of at least one hour. This CRL will contain the revoked, if any, certificates for **OWGTM** end-users / subscribers.

For the specific case of SSL 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** provide an OCSP service that is available on a 24x7 basis. The OCSP service availability is not mandatory for low assurance certificates, as the "CertifyID Standard Personal Certificate".

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 SSL certificates, **OWGTM** will ensure compliance with the applicable Baseline and/or Extended Validation requirements from the CA/Browser Forum.

4.9.10 On-line revocation checking requirements

On-line revocation checking is openly provided without restriction to all Participants in the PKI.

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 regarding 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.

4.9.13 Circumstances for suspension

Suspension is only supported for Personal Certificates.

Persons allowed according to 4.9.14, can explicitly request the suspension of their certificates, their will being sufficient justification.

4.9.14 Who can request suspension

See section 4.9.2.

4.9.15 Procedure for suspension request

See section 4.9.3. The procedure allows subscribers to request certificate suspension.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate Status Services

OWGTM provides 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.

Other services could be available, as stipulated in the corresponding End User Agreement.

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

Only the Escrow of end-user certificates is allowed. For infrastructure certificates, as CA, RA or others, appropriate back-up policies must be implemented, according to section 6.2.4.

4.12.1 Key escrow and recovery policy and practices

The **OWGTM** doesn't stipulate how the end-user private keys can be escrowed or recovered, nor provides such facilities in direct commercial services to end-users. Corporate Issuing CAs or RAs accessing through a "Managed PKI" interface, can implement different procedures for key escrow, being mandatory in such case an explicit communication of such features to the certificate subscriber.

In particular, **OWGTM** doesn't recommend any type of escrow or back-up of private keys enabled for digital signatures, provided that the end-user is the sole entity having effective access to this information.

4.12.2 Session key encapsulation and recovery policy and practices

If Key Escrow is implemented, according to the previous sections, any session key enabling the decryption of a private key must be kept under sole control of the certificate subscriber or authorized representative.

5 Management, Operational, and Physical Controls

This section describes the non-technical security controls used by the participants[5] 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.wisekey.com/repository).

The **OWGTM** allows third parties to host and operate[6] some of the components of its infrastructure. If such a delegation occurs, the assigned party will be requested to meet the controls stipulated in this section and an auditing process will be executed to ensure that the necessary measures to ensure these controls are effective are in place and enforced.

In particular:

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

5.1 Physical Security Controls

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

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] The security requirements for subscribers and relying parties are described in their particular agreements. These agreements could stipulate different controls depending on the Certificate Policy and they are published in the **OWGTM** website (http://www.wisekey.com/repository).
[6] Critical operations are not allowed to be outsourced. In particular, Key Ceremonies are not allowed to be delegated in any case, and must always be executed by the Certification Authority issuing the subordinated CA's Certificate.

5.1.3 Power and air conditioning

The facilities are equipped with uninterrupted power supplies (UPS) with enough capacity to autonomously maintain the **OWGTM** systems during electric power outages and protect these systems from damage that may result from power fluctuations.

The air-conditioning systems used in the **OWGTM** are composed of redundant independent equipment that ensures the operative margins in temperature and humidity inside the Secure Datacenter.

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

The facilities implement fire detection, prevention and protection controls.

5.1.6 Media storage

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

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

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

5.1.7 Waste disposal

The disposal of optical or magnetic media and paper containing any information generated during **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 Backup

On a daily basis, **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.

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

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

5.2.2 Number of persons required per task

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

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

5.2.3 Identification and authentication for each role

All the persons assuming a role in the **OWGTM** systems[7] 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

Roles requiring Separation of duties include at least the following:

- Enabling a CA into a production status (CA Ceremony procedures)
- Issuance, or revocation of CA Certificates
- Validation of information and issuance of high assurance subscriber certificates

5.3 Personnel Security 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.

[7]See note 5

- 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.

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

If an unauthorized action is detected the **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.

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 to at least the following information:

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

- Incident response procedures

5.3.9 Contract termination and assigned role change procedures

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

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

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

5.4 Audit Logging Procedures

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

5.4.1 Types of events recorded

OWGTM records in their servers all events related to:

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

5.4.2 Frequency of processing log

Logs are processed and audited in a regular basis.

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

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log

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

The destruction of an audit record can only executed after signed authorization from the **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 executes regular vulnerability assessment by monitoring the activity logs. 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.

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

5.5 Records Archival

This section includes the stipulations regarding record retention policies.

5.5.1 Types of records archived

The information and events archived are:

- Information generated (at CA and RA) during the life cycle of all **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 during a 7-year period.

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 encrypted and remotely 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 need 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.

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

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

If the hardware or software resources are altered or suspected to have been altered, the **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:

- Notify all certificate subscribers and 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 dependant of that Root CA.

6 Technical Security Controls

This section describes the measures taken by Certification Authorities operating under the **OWGTM**[8]. 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.wisekey.com/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

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 auditor[9].
- 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.

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

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

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

6.1.2 Private key delivery to subscriber

In the **OWGTM** trust model the specific end-entity certificate profiles allow the generation of the private key by the Registration Authority or by the end-user Subscriber. If the keys are generated by the Registration Authority, FIPS 140-1 Level 1, or higher, containers must be used. In particular, the usage of password-protected encrypted software files, or smartcards or other valid crypto-tokens is accepted.

---

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

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 CSR standards.

6.1.4 CA public key delivery to relying parties

The public keys of all Certification Authorities operating under the **OWGTM** Trust Model are published and can be freely downloaded from its repository which is located at http://www.wisekey.com/repository.

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 and ECC NIST P-256, P-384, or P-

521 key pairs at all levels of the hierarchy.

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

6.1.6 Public key parameters generation and quality checking

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

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

All 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 7.1.2.

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.

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

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 encryption end-user certificates, as described in section 4.12.

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 typically 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 4.12.

6.2.5 Private key archival

The Private Keys are never archived for any PKI participant.

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

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

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

6.2.8 Method of activating private key

The private key in Certification Authorities in the **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 (smartcard or other accepted crypto-tokens) from the workstation it is used.

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

6.2.10 Method of destroying private key

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

- Private Key is no longer used.
- 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
OWGTM Root CA GB (SHA-2)	25 years
Policy Certification Authority	Up to the entire life time of the Root CA upon issuance
Issuing Certification Authority	Up to 10 years
End-Entity Certificate	Up to 3 years

It must be understood that the validity period of a certificate can be limited by the own validity of the issuing Certification Authority, as is not permitted that a subordinate entity extends its validity beyond the issuer.

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

6.4 Activation Data

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

6.4.1 Activation data generation and installation

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

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

End entity activation data, is only stipulated for hardware-based private-keys. In particular:

- Private Keys for RA and Qualified Certificates will be 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 "CertifyID 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 the people involved in the **OWGTM** 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.

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:

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

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

6.5.2 Computer security rating

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

6.6 Life Cycle Security Controls

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

6.6.1 System development controls

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

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

6.6.2 Security management controls

The **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

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

6.7 Network Security Controls

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

In particular, the server used for the **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.

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.wisekey.com/repository.

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

7 Certificate and CRL Profiles

All certificates issued under the **OWGTM** Trust Model are compliant to:

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

This section of the CPS is provided for general stipulation and as a reference to the specific Certificate Policy for each certificate type, available in Annex B: Approved Certificate Policies and Profiles.

7.1 Certificate Profile

The current list of approved Certificate Policies, and its associated profile is available in Annex B: Approved Certificate Policies and Profiles.

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

Certificate extensions are disclosed in the tables available in Annex B: Approved Certificate Policies and Profiles.

7.1.3 Algorithm object identifiers

Certificates issued under the **OWGTM** can use alternatively SHA-1 or SHA-2. The Algorithm object identifiers are:

- **sha256withRSAEncryption**:
  ```
  OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)
  rsadsi(113549) pkcs(1) pkcs-1(1) 11}
  ```
- **sha-1WithRSAEncryption**:
  ```
  OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)
  rsadsi(113549) pkcs(1) pkcs-1(1) 5}
  ```
- Where appropriate, algorithm identifiers related to ECC will be applied

7.1.4 Name forms

Certificates issued under the **OWGTM** contain the "Distinguished Name", in X.500 format, for the issuer and the subscriber, set in the fields "Issuer Name" and "Subject Name" respectively, and are formed as defined in section 3.1.

7.1.5 Name constraints

Issuing Certification Authorities not operated by WISeKey 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 MPKI RA Interface for Certificate Requests for corporations having access to a dedicated Registration Authority.

7.1.6 Certificate policy object identifier

The specific policy OID for each certificate profile, if used, is documented in Annex B: Approved Certificate Policies and Profiles.

7.1.7 Usage of Policy Constraints extension

Issuing Certification Authorities not operated by WISeKey are appropriately constrained to be compliant with CA/Browser Forum requirements. These 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

This information is available in Annex B: Approved Certificate Policies and Profiles.

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 1 and Version 2 are supported in the **OWGTM**.

7.2.2 CRL Profile and CRL entry extensions

The generic CRL profile is specified in the following table:

Version	*1 (i.e. X.509 version 2 CRL)*
Serial Number	*Unique serial numbers are assigned by the CA*
Signature Algorithm	SHA1RSA
Issuer Distinguished Name	
Common Name (CN)	<CA-NAME>
Organisational Unit (OU)	(As defined for the CA)
Organisational Unit (OU)	(As defined for the CA)
Organisation (O)	(As defined for the CA)
Country (C)	(As defined for the CA)
This update	Date/Time of issue
Next update	(As appropriate for the CA, stipulated in section 4.9.7)
Revoked certificates	
Serial number	<Subscriber certificate serial number>
Revocation date	<Time/date certificate marked revoked>
CRL reason code	<In accordance with RFC3280>
CRL number	Unique number for each CRL issued by CA Extension marked non-critical.

Authority Key Identifier	Extension marked non-critical.
Key Identifier	<CA-KeyID>

If any specific consideration must be stipulated for a particular Certificate Policy, this is specified in Annex B: Approved Certificate Policies and Profiles.

7.3 OCSP Profile

In general, the status of all certificates in the **OWGTM**, except the "CertifyID Standard Personal Certificate" can be validated by sending requests compliant with RFC 2560.

OWGTM ensures compliance with any applicable requirement from the CA/Browser Forum in terms of OCSP implementations.

7.3.1 Version number(s)

OWGTM provides support for Version 1 of RFC2560 and RFC5019.

7.3.2 OCSP extensions

If a Certificate Policy mandates the support of OCSP, the appropriate AIA extension will be included in the affected certificates, specifying the URL of the OCSP responder server.

If any specific consideration must be stipulated for a particular Certificate Policy, this is specified in Annex B: Approved Certificate Policies and Profiles.

8 Compliance Audit and Other Assessment

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.

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.

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 two levels of audit and accreditation.

- The Root CA, Policy CAs and Issuing CAs owned or operated by WISeKey. These services are audited against the WebTrust criteria and commonly accepted industry accreditation standards. Issuing CAs operated by third parties which don't enforce name constraints must be included in this assessment.
- The Issuing CAs owned and/or operated by third parties enforcing name constraints. 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.

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
- 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** Repository.

9 Other Business and Legal Matters

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

For the CPS only generic stipulations are included, the reader is required to check the appropriate Certificate Policy document and corresponding Terms and Conditions.

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, WISeKey doesn'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, WISeKey doesn't apply fees on the access to certificate information made public in the different repositories.

9.1.4 Fees for other services

WISeKey, as operator of 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" 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 insurance contract that covers the liability expressed in section 9.8.

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

9.2.2 Other assets

No stipulations.

9.2.3 Insurance or warranty coverage for end-entities

The maximum per certificate liability of the OISTE WISeKey Root PKI or any other entity within the OISTE WISeKey Root PKI shall be established in the applicable Certificate Policy. Such per certificate liability limit shall apply regardless of the number of transactions, digital signatures, or causes of action arising out of or related to such certificate or any services provided in respect of such certificate and on a cumulative basis.

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 "EXTRICTLY CONFIDENTIAL" when generated or exchanged among involved parties.

9.3.2 Information not within the scope of confidential information

The following information shall be deemed as non-confidential:

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

9.3.3 Responsibility to protect confidential information

The **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 Privacy Policy of the **OWGTM** is published at the URL http://www.wisekey.com/repository. This Policy is compliant with the applicable requirements for international commercial services, and specifically with any applicable requirements from the CA/Browser Forum.

9.4.1 Privacy plan

Personal Information communicated to the **OWGTM** by the certificate subscribers is stored in a database owned by the operator of the Certification and/or Registration Authority. This database is conveniently protected to avoid any unauthorized access or modification.

The subscribers will have the right to access their information and request its modification or cancellation. These rights can be exercised by written request at the e-mail address published in section 1.5.2 of this document.

In the course of its duties the **OWGTM** Issuing Certification Authorities operated by WISeKey need to electronically store and process personal data. All such actions must be performed in accordance with Swiss laws related to data security and privacy and Electronic Signature. Furthermore, all provisions of section 9.3 apply.

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 **OWGTM** is required to obtain the consent to use the subscriber's personal information.

This consent is understood by the acceptance of the "Terms and Conditions" and/or "End User Agreement" by the subscriber. This acceptance is recognised 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 under the **OWGTM**, Object Identifiers, the CPS and the different CP are owned by the **OWGTM**.

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
- Utilise 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.
- An obligation and warranty that it will not install and use the Certificate(s) until it has reviewed and verified the accuracy of the data in each Certificate.
- An obligation and warranty to install the Certificate only on the server accessible at the domain name listed on the Certificate, and to use the Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement.
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS.
- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created.
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.
- An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request that the Certification Authority revokes the Certificate, in the event that: (a) any information in the Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key listed in the Certificate.
- An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an Certificate upon expiration or revocation of that Certificate.

The "Subscriber agreement" could include additional warranties.

9.6.4 Relying party representations and warranties

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

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

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

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

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

The "Relying party agreement" could include additional warranties.

9.6.5 Representations and warranties of other participants

No stipulations.

9.7 Disclaimers of Warranties

Other Disclaimer of warranties (if existing) is included as part of the agreement presented to each PKI participant.

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, WISeKey'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).

9.9 Indemnities

Indemnities 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.

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

9.11 Individual notices and communications with participants

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

9.12 Amendments

The **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.wisekey.com/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** will 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 will be modified to reflect a change of major version of the document.

9.13 Dispute Resolution Procedures

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

9.14 Governing Law

The CP, the CPS and the operations of the **OWGTM** are all governed by the laws of 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 for 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.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

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

9.17 Other Provisions

No stipulations.

10 Annex A: Glossary

This document makes use of the following defined terms:

Activation data - Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share).

Authentication - The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what hey claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.

CA-certificate - A certificate for one CA's public key issued by another CA.

Certificate policy (CP) - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Certification path - An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS) - A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

CPS Summary (or CPS Abstract) - A subset of the provisions of a complete CPS that is made public by a CA.

Identification - The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes:

(1) Establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and
(2) Establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Issuing certification authority (issuing CA) - In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Participant - An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

PKI Disclosure Statement (PDS) - An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.

Policy qualifier - Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information.

Registration authority (RA) - An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [Note: The term Local Registration Authority (LRA) is sometimes used in other documents for the same concept.]

Relying party - A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Relying party agreement (RPA) - An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates.

Set of provisions - A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in this framework.

Subject certification authority (subject CA) - In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing certification authority).

Subscriber - A subject of a certificate who is issued a certificate.

Subscriber Agreement - An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

Validation - The process of identification of certificate applicants. "Validation" is a subset of "identification" and refers to identification in the context of establishing the identity of certificate applicants.

10.1 Table of Acronyms

CP Identifier	Process
AICPA	American Institute of Certified Public Accountants. ANSI The American National Standards Institute
ACS	Authenticated Content Signing
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Instituted of Chartered Accountants CP Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
EV	Extended Validation
FIPS	United State Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
ICC	International Chamber of Commerce
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
KRB	Key Recovery Block
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PCA	Primary Certification Authority
PIN	Personal identification number
PKCS	Public-Key Cryptography Standard
KRB	Key Recovery Block
OID	Object Identifier
OWGTM	OISTE / WISeKey Global Trust Model
PCA	Policy Certification Authority
PIN	Personal identification number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PAA	Policy Approval Authority
RA	Registration Authority
RFC	Request for comment
SAR	Security Audit Requirements
S/MIME	Secure multipurpose Internet mail extensions
SSL	Secure Sockets Layer
TLD	Top-Level Domain

11 Annex B: Approved Certificate Policies and Profiles

The profiles of certificates that are issued by the CA are detailed below.

The characteristics of the attributes are marked as follows:

- m : mandatory attribute
- o: optional attribute
- e: editable attribute value
- f: fix attribute value

11.1 Issuing CAs and Certificate Policies binding

Issuing CAs under the OWGTM must mandatorily include one of the class identifiers "Standard", "Advanced" or "Qualifier" in its Common Name. According to this identifier, the CP that are bound to each class is specified in the following table:

CA Class	*Allowed Certificate Policies*
Standard	*11.2.1 CertifyID Standard Personal Certificate*
Advanced	*11.2.2 CertifyID Advanced Personal Certificate* *11.3.1 CertifyID Standard SSL Certificate* *11.3.2 CertifyID Advanced OV SSL Certificate* *11.3.3 CertifyID Advanced EV SSL Certificate*
Qualified	*11.2.3 CertifyID Qualified Personal Certificate* 11.3.4 CertifyID Qualified Corporate Certificate

11.2 Personal Certificates

11.2.1 CertifyID Standard Personal Certificate

Version	*2 (i.e. X.509 version 3)*	
Serial Number	*Unique serial numbers are assigned by the CA*	
Signature Algorithm	Sha1RSA or Sha2RSA	f
Issuer Distinguished Name		
Common Name (CN)	<Issuer CA Name>	f
Organisational Unit (OU)	<Optional>	f
Organisational Unit (OU)	<Optional>	f
Organisation (O)	<Issuer-Organization>	f
Country (C)	<Issuer-Country>	f
Validity		
Not Before	Time of issue	
Not After	1 – 3 years	f
Subject		
Email (E)	<Subscriber email>	m/e
Common Name (CN)	<Subscriber common name>	o/e
Locality (L)	<Subscriber locality>	o/e
State or Province Name (ST)	<Subscriber state>	o/e
Organisational Unit (OU)	<Optional> "CertifyID Standard User"	o/f
Organisational Unit (OU)	<Optional>	o/e
Organisational Unit (OU)	Validated by [Appointed RA] – CertifyID RA	o/f

	Issued via [Client MPKI Subscriber Name]	
Organisational Unit (OU)	<Optional, Subscriber organisational unit>	o/e
Organization (O)	<Optional, Subscriber organization>	o/e
Country (C)	<Subscriber country code>	m/e
Subject Public Key Info	2048 bit RSA	f

x.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	<KeyID>
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
SMIME Capabilities (optional)	[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80 [3]SMIME Capability Object ID=1.3.14.3.2.7 [4]SMIME Capability Object ID=1.2.840.113549.3.7
CRL Distribution Point	Extension marked non-critical.
Full name	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=<URL-TO-CRL>
Policy Qualifier	(See Annex D: Policy Qualifiers)
Authority Information Access	Extension marked non-critical.
Extensions	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<URL-TO-ISSUER-CERT>
Key Usage	Extension marked critical.
Allowed Key Usages	Digital Signature, Key Encipherment, Data Encipherment (f0)
Allowed Enhanced Key Usages	Document Signing (1.3.6.1.4.1.311.10.3.12) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)

11.2.2 CertifyID Advanced Personal Certificate

Version	*2 (i.e. X.509 version 3)*	
Serial Number	*Unique serial numbers are assigned by the CA*	
Signature Algorithm	Sha1RSA or Sha2RSA	f
Issuer Distinguished Name		
Common Name (CN)	<Issuer CA Name>	f
Organisational Unit (OU)	<Optional>	f
Organisational Unit (OU)	<Optional>	f
Organisation (O)	<Issuer-Organization>	f

Country (C)	<Issuer-Country>	f
Validity		
Not Before	Time of issue	
Not After	1 – 3 years	f
Subject		
Email (E)	<Subscriber email>	m/e
Common Name (CN)	<Subscriber common name, juridic persons allowed>	m/e
Locality (L)	<Subscriber locality>	o/e
State or Province Name (ST)	<Subscriber state>	o/e
Organisational Unit (OU)	<Optional> "CertifyID Advanced User"	o/f
Organisational Unit (OU)	<Optional>	o/e
Organisational Unit (OU)	Validated by [Appointed RA] – CertifyID RA Issued via [Client MPKI Subscriber Name]	o/f
Organisational Unit (OU)	<Optional, Subscriber organisational unit>	o/e
Organization (O)	<Optional, Subscriber organization>	o/e
Country (C)	<Subscriber country code>	m/e
Subject Public Key Info	2048 bit RSA	f

x.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	<KeyID>
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
SMIME Capabilities (optional)	[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80 [3]SMIME Capability Object ID=1.3.14.3.2.7 [4]SMIME Capability Object ID=1.2.840.113549.3.7
CRL Distribution Point	Extension marked non-critical.
Full name	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=<URL-TO-CRL>
Policy Qualifier	(See Annex D: Policy Qualifiers)
Authority Information Access	Extension marked non-critical.
Extensions	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<URL-TO-ISSUER-CERT>
Key Usage	Extension marked critical.
Allowed Key Usages	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
Allowed Enhanced Key Usages	Document Signing (1.3.6.1.4.1.311.10.3.12)

	Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)

11.2.3 CertifyID Qualified Personal Certificate

Version	*2 (i.e. X.509 version 3)*	
Serial Number	*Unique serial numbers are assigned by the CA*	
Signature Algorithm	Sha1RSA or Sha2RSA	f
Issuer Distinguished Name		
Common Name (CN)	<Issuer CA Name>	f
Organisational Unit (OU)	<Optional>	f
Organisational Unit (OU)	<Optional>	f
Organisation (O)	<Issuer-Organization>	f
Country (C)	<Issuer-Country>	f
Validity		
Not Before	Time of issue	
Not After	1 – 3 years	f
Subject		
Email (E)	<Subscriber email>	m/e
Common Name (CN)	<Subscriber common name>	m/e
Locality (L)	<Subscriber locality>	o/e
State or Province Name (ST)	<Subscriber state>	o/e
Organisational Unit (OU)	<Optional> "CertifyID Qualified User"	o/f
Organisational Unit (OU)	<Optional>	o/e
Organisational Unit (OU)	Validated by [Appointed RA] – CertifyID RA Issued via [Client MPKI Subscriber Name]	o/f
Organisational Unit (OU)	<Optional, Subscriber organisational unit>	o/e
Organization (O)	<Optional, Subscriber organization>	o/e
Country (C)	<Subscriber country code>	m/e
Subject Public Key Info	2048 bit RSA	f

x.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	<KeyID>
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
SMIME Capabilities (optional)	[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80 [3]SMIME Capability Object ID=1.3.14.3.2.7 [4]SMIME Capability Object ID=1.2.840.113549.3.7
CRL Distribution Point	Extension marked non-critical.
Full name	[1]CRL Distribution Point

	Distribution Point Name: Full Name: URL=<URL-TO-CRL>
Policy Qualifier	(See Annex D: Policy Qualifiers)
Authority Information Access	Extension marked non-critical.
Extensions	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<URL-TO-ISSUER-CERT>
Key Usage	Extension marked critical.
Allowed Key Usages	Digital Signature, Key Encipherment, Data Encipherment (f0)
Allowed Enhanced Key Usages	Document Signing (1.3.6.1.4.1.311.10.3.12) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)

11.3 Corporate and Server Certificates

11.3.1 CertifyID Standard SSL Certificate

Version	*2 (i.e. X.509 version 3)*	
Serial Number	*Unique serial numbers are assigned by the CA*	
Signature Algorithm	Sha1RSA or Sha2RSA	f
Issuer Distinguished Name		
Common Name (CN)	<Issuer CA Name>	f
Organisational Unit (OU)	<Optional>	f
Organisational Unit (OU)	<Optional>	f
Organisation (O)	<Issuer-Organization>	f
Country (C)	<Issuer-Country>	f
Validity		
Not Before	Time of issue	
Not After	1 – 3 years	f
Subject		
Common Name (CN)	<Subscriber common name>	m/e
Locality (L)	<Subscriber locality>	o/e
State or Province Name (ST)	<Subscriber state>	o/e
Country (C)	<Subscriber country code>	m/e
Subject Public Key Info	2048 bit RSA	f
SubjectAltName	<List of SAN> (at least one)	m/e

x.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	<KeyID>
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
CRL Distribution Point	Extension marked non-critical.
Full name	[1]CRL Distribution Point Distribution Point Name: Full Name:

	URL=<URL-TO-CRL>	
Policy Qualifier	(See Annex D: Policy Qualifiers)	
Authority Information Access	Extension marked non-critical.	
Extensions	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<URL-TO-ISSUER-CERT>	
Key Usage	Extension marked critical.	
Value	Digital Signature, Key Encipherment (a0)	

11.3.2 CertifyID Advanced OV SSL Certificate

Version	*2 (i.e. X.509 version 3)*	
Serial Number	*Unique serial numbers are assigned by the CA*	
Signature Algorithm	Sha1RSA or Sha2RSA	f
Issuer Distinguished Name		
Common Name (CN)	<Issuer CA Name>	f
Organisational Unit (OU)	<Optional>	f
Organisational Unit (OU)	<Optional>	
Organisation (O)	<Issuer-Organization>	f
Country (C)	<Issuer-Country>	f
Validity		
Not Before	Time of issue	
Not After	1 – 3 years	f
Subject		
Common Name (CN)	<Subscriber common name>	m/e
Organisation (O)	<Subscriber organisational affiliation>	m/e
Locality (L)	<Subscriber locality>	o/e
State or Province Name (ST)	<Subscriber state>	o/e
Country (C)	<Subscriber country code>	m/e
Subject Public Key Info	2048 bit RSA	f
SubjectAltName	<List of SAN> (at least one)	m/e

x.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	<KeyID>
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
CRL Distribution Point	Extension marked non-critical.
Full name	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=<URL-TO-CRL>
Policy Qualifier	(See Annex D: Policy Qualifiers)
Authority Information Access	Extension marked non-critical.
Extensions	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name:

	URL=<URL-TO-ISSUER-CERT>
Key Usages	Extension marked critical.
Values	Key Usage: Data Encipherment, Digital Signature, Key Encipherment Extended Key Usage: Client Authentication, Server Authentication Netscape Certificate Type (optional): SSL Client, SSL Server

11.3.3 CertifyID Advanced EV SSL Certificate

Version	*2 (i.e. X.509 version 3)*	
Serial Number	*Unique serial numbers are assigned by the CA*	
Signature Algorithm	Sha1RSA or Sha2RSA	f
Issuer Distinguished Name		
Common Name (CN)	<Issuer CA Name>	f
Organisational Unit (OU)	<Optional>	f
Organisational Unit (OU)	<Optional>	
Organisation (O)	<Issuer-Organization>	f
Country (C)	<Issuer-Country>	f
Validity		
Not Before	Time of issue	
Not After	1 year	f
Subject		
Common Name (CN)	<Subscriber common name>	m/e
BusinessCategory	<Type of organization>	m/e
Organisation (O)	<Subscriber organisational affiliation>	m/e
StreetAddress	<Street of the organization>	m/e
Locality (L)	<Subscriber locality>	o/e
State or Province Name (ST)	<Subscriber state>	o/e
Country (C)	<Subscriber country code>	m/e
Subject Public Key Info	2048 bit RSA	f
SubjectAltName	<List of SAN> (at least one)	m/e

x.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	<KeyID>
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
CRL Distribution Point	Extension marked non-critical.
Full name	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=<URL-TO-CRL>
Policy Qualifier	(See Annex D: Policy Qualifiers)
Authority Information Access	Extension marked non-critical.
Extensions	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<URL-TO-ISSUER-CERT>
Key Usages	Extension marked critical.

Values	Key Usage: Data Encipherment, Digital Signature, Key Encipherment Extended Key Usage: Client Authentication, Server Authentication Netscape Certificate Type (optional): SSL Client, SSL Server

11.3.4 CertifyID Qualified Corporate Certificate

Version	*2 (i.e. X.509 version 3)*	
Serial Number	*Unique serial numbers are assigned by the CA*	
Signature Algorithm	Sha1RSA or Sha2RSA	f
Issuer Distinguished Name		
Common Name (CN)	<Issuer CA Name>	f
Organisational Unit (OU)	<Optional>	f
Organisational Unit (OU)	<Optional>	
Organisation (O)	<Issuer-Organization>	f
Country (C)	<Issuer-Country>	f
Validity		
Not Before	Time of issue	
Not After	1 – 3 years	f
Subject		
Email (E)	<Subscriber email>	m/e
Common Name (CN)	<Organization / Representative names>	m/e
Locality (L)	<Subscriber locality>	o/e
State or Province Name (ST)	<Subscriber state>	o/e
Organisational Unit (OU)	<Optional> “CertifyID Qualified Organization”	o/f
Organisational Unit (OU)	<Optional>	o/e
Organisational Unit (OU)	Validated by [Appointed RA] – CertifyID RA Issued via [Client MPKI Subscriber Name]	o/f
Organisational Unit (OU)	<Optional, Subscriber organisational unit>	o/e
Organization (O)	<Optional, Subscriber organization>	o/e
Country (C)	<Subscriber country code>	m/e
Subject Public Key Info	2048 bit RSA	f

x.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	<KeyID>
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
SMIME Capabilities	[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80 [3]SMIME Capability Object ID=1.3.14.3.2.7 [4]SMIME Capability Object ID=1.2.840.113549.3.7
CRL Distribution Point	Extension marked non-critical.

Full name	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=<URL-TO-CRL>
Policy Qualifier	(See Annex D: Policy Qualifiers)
Authority Information Access	Extension marked non-critical.
Extensions	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<URL-TO-ISSUER-CERT>
Key Usage	Extension marked critical.
	Digital Signature, Key Encipherment, Data Encipherment (f0)
Allowed Enhanced Key Usages	Document Signing (1.3.6.1.4.1.311.10.3.12) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)

11.4 Infrastructure Certificates

11.4.1 Issuing CA Certificate

Version	*2 (i.e. X.509 version 3)*	
Serial Number	*Unique serial numbers are assigned by the upper level CA*	
Signature Algorithm	Sha1RSA or Sha2RSA	f
Issuer Distinguished Name		
Distinguished Name (DN)	<Upper level CA DN>	f
Validity		
Not Before	Time of issue	
Not After	Not after the validity of the upper level CA	f
Subject		
Common Name (CN)	<Issuing CA Name>	m/e
Organization (O)	<CA owner organization>	o/e
Country (C)	<CA owner country code>	m/e
Subject Public Key Info	2048 bit RSA	f

x.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	<KeyID>
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
Key Usage	Extension marked critical.
Values	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Basic Constraints	CA=TRUE PATHLENCONSTRAINTS=0
Name Constraints	<LIST OF NAME CONSTRAINTS>
Certificate Policies	[1]Certificate Policy: [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier:

	11.4.1.1.1.1 Notice Text=Only for authorized uses. Seulement pour des usages autorises. Solo para usos autorizados. WISeKey SA Copyright (c) 2005 11.4.1.1.1.2 [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.wisekey.com/repository [2]Certificate Policy: Policy Identifier=<anyPolicy> (CA Operated by WISeKey) OR <2.16.756.5.14.7.3> (CA not operated by WISeKey)
CRL Distribution Point	Extension marked non-critical.
Full name	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=<URL-TO-CRL>
Authority Information Access	Extension marked non-critical.
Extensions	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<URL-TO-ISSUER-CERT>
Allowed Enhanced Key Usages	Document Signing (1.3.6.1.4.1.311.10.3.12) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)

11.4.2 CertifyID URA Admin Certificate

Admin Certificates are technically equivalent to the Advanced Personal Certificates.

It is admitted to use the certificate profiles for enrolment agent, built-in in the Certificate Management Solution (e.g. “Enrolment Agent” profile for the Microsoft Certificate Services).

11.4.3 CertifyID OCSP Certificate

As defined by the incumbent RFC. WISeKey ensures compliance with regulations made public by the CA/Browser Forum, as appropriate for online status services.

11.4.4 CertifyID TSA Certificate

Version	*2 (i.e. X.509 version 3)*	
Serial Number	*Unique serial numbers are assigned by the CA*	
Signature Algorithm	Sha1RSA / Sha2RSA	f
Issuer Distinguished Name		
Common Name (CN)	WISeKey CertifyID Advanced Services CA 1	f
Organisational Unit (OU)	International	f
Organisational Unit (OU)	Copyright (c) 2006 WISeKey SA	
Organisation (O)	WISeKey	f
Country (C)	CH	f
Validity		
Not Before	Time of issue	

Not After	Not after the expiry date of the Issuing CA	f
Subject		
Common Name (CN)	<Subscriber common name>	m/e
Organisational Unit (OU)	<Copyright notice>	m/f
Organisational Unit (OU)	CertifyID Advanced TSA Server	m/f
Organisational Unit (OU)	Validated by [Appointed RA] – CertifyID RA Issued via [Client MPKI subscriber name]	m/e
Organisation (O)	<Subscriber organisational affiliation>	m/e
Locality (L)	<Subscriber locality>	o/e
State or Province Name (ST)	<Subscriber state>	o/e
Country (C)	<Subscriber country code>	m/e
Subject Public Key Info	2048 bit RSA	f

x.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	<KeyID>
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
CRL Distribution Point	Extension marked non-critical.
Full name	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=<URL-TO-CRL>
Authority Information Access	Extension marked non-critical.
Extensions	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<URL-TO-ISSUER-CERT>
Key Usage	Extension marked critical.
Value	Digital Signature, Key Encipherment (a0)
Allowed Enhanced Key Usages	Time Stamping (1.3.6.1.5.5.7.3.8)

12 Annex C: Identity Validation Policies

12.1 Validation process for subordinate Certification Authorities

To issue a CertifyID Subordinate CA license, WISeKey will follow an internal approved procedure to verify an applicant's identity. The submission and validation procedure includes the following steps:

- Submission of subordinate CA applicant data
- Submission of organisation identity documents
- Submission of individual identity documents of proposed CA administrator(s) and organisation's directors, including letters of appointment of CA administrator(s)
- Submission of signed EUA by CA administrator(s)
- Identity Verification and Validation
- Submission of signed contract to WISeKey – stipulating adherence to terms and conditions of usage, obligation to respect WISeKey CPS & CP, and other conditions thereof.
- Submission of pre-issuance audit statement of fulfilment of contract and security requirements
- Submission of certificate request
- Validation of certificate request and license validation - resulting in Denial or Issuance of the CA certificate
- Installation and Post-Audit – including verification of contract compliance, and CRL publishing

To verify and validate the identity of an applicant, WISeKey will collect all documents used for the license approval process, which involves verifying the following:

- That any individual(s) involved in the process are who they purport to be
- That the organization exists and is registered in one or more countries
- That the individual(s) representing the organization has the authority to do so.
- That the nominated CA Administrator requesting a subordinate CA certificate has been given authority to do so by the organization
- That the individual and organization can be located by telephone and by post and has a third party reference that makes its reputable as a trusted entity
- That the domain name(s) for which the organization will be allowed to issue certificates are registered to the organization, or that they have been given permission to use them by the registered owner

WISeKey needs the duly registered statutes or by-laws, together with the registered physical address. In the case of entities that are not registered in the trade registry, other similar documents are also acceptable (e.g. official documents of public entities, notaries, etc.).

Subordinate CA certificates contain naming and domain name constraints, thus commercial registrar records are used to validate Internet Domain Names. The organisation name and address must match the business incorporation papers of the organisation, or the latest data available from the Business Register. A call back must be performed to verify that the individuals with authority in the application work with the organisation, using a telephone number found through public directory services. If its administered by another applicant on behalf of the organisation owning the domain, then a signed letter from the organisation owning the domain must be received granting the certificate applicant the right to use the domain name in their certificates.

12.2 Validation policies for subscriber certificates

12.2.1 Personal Certificates

CP Identifier	Validation Policy
CertifyID Standard Personal Certificate	**ID Data Verified**: Basic data is verified such as the email address; or in the case of an organisation ownership of the domain names in the certificate, with responsibility to verify the individual entities to which certificates are issued. **Method of Verification**: ▪ Bounce back email verification procedure proving access to the email account is accepted. ▪ Database (such as existing HR, or IDM) of organisation, with details of organisation's users. ▪ Commonly accepted business methods of identity verification. **Entities authorized to verify**: ▪ The entity purchasing and managing the e-ID system under contract with WISeKey. ▪ Authorised internal entity (e.g. human resources dept.) or external entity who is legally bound to comply with the verification procedures.
CertifyID Advanced Personal Certificate	**ID Data Verified**: Personal identity data such as name, date of birth, nationality, 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. There's an obligation to verify the identity of real physical and juridical persons names included in the certificates. **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. **Entities authorized to verify**: ▪ Authorised internal entity (e.g. human resources dept.) or external entity who is legally bound to comply with the verification procedures. ▪ The entity purchasing and managing the e-ID system under contract with WISeKey.
CertifyID Qualified Personal Certificate	**ID Data Verified**: Personal identity data such as name, date of birth, nationality, 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. If local law compliance intended, then local law requirements apply and override. **Method of Verification**: Face to face or direct verification but may be done through database of identity data that is well-maintained and was created based on face to face or direct verification using primary ID documents. If local law compliance intended, then local law requirements apply and override. **Entities authorized to verify**: ▪ Authorised internal entity (e.g. human resources dept.) or external entity who is legally bound to comply with the verification procedures. ▪ The entity purchasing and managing the e-ID system under contract with WISeKey. ▪ If local law compliance intended, then local law requirements apply and override.

12.2.2 Corporate and Server Certificates

CP Identifier	Validation Policy
CertifyID Standard SSL[10] Certificate	**ID Data Verified**: Identification data of the Server, as defined by the Baseline Requirements of the CA/Browser Forum for SSL Certificates. **Method of Verification**: The identification data included in the certificate are verified according to the Baseline Requirements made public by the CA/Browser Forum. **Entities authorized to verify**: ▪ Authorised internal entity (Registration Authority.) or external entity that is legally bound to comply with the verification procedures. ▪ The entity purchasing and managing the e-ID system under contract with WISeKey.
CertifyID Advanced OV SSL Certificate	**ID Data Verified**: Same data than CertifyID Standard SSL Certificate, including the Identity of the Organization, which is included in the subject name of the certificate.

[10] Note: SSL Certificates can be offered in different versions (e.g. Wildcard or Unified Communications), but always according to the applicable base CP and CA/Browser Forum requirements.

	Method of Verification: In addition to the methods indicated for Standard SSL certificates, the identity of the organization is validated according to the Baseline Requirements published by the CA/Browser forum, in what concerns to Organization validation. **Entities authorized to verify**: ▪ Authorised internal entity (Registration Authority.) or external entity that is legally bound to comply with the verification procedures. ▪ The entity purchasing and managing the e-ID system under contract with WISeKey.
CertifyID Advanced EV SSL Certificate	**ID Data Verified**: Equivalent to the Advanced OV Certificates, adapted to be compliant to the requirements for EV certificates, as defined by the CA/Browser Forum. **Method of Verification**: The identification data included in the certificate are verified according to the Extended Validation Requirements made public by the CA/Browser Forum. **Entities authorized to verify**: ▪ Authorised internal entity (Registration Authority.) or external entity that is legally bound to comply with the verification procedures. ▪ The entity purchasing and managing the e-ID system under contract with WISeKey.
CertifyID Qualified Corporate Certificate	**ID Data Verified**: Legal entities are required to provide relevant official documentation. If the name of physical persons are included in the certificate, as legal representatives of the organization, it is required to fulfil a complete identification of the person and it's legal attribution to act as representative. Verification of device or other type of entity or object is done with substantially equivalent data. If local law compliance intended, then local law requirements apply and override. **Method of Verification**: Face to face or direct verification but may be done through database of identity data that is well-maintained and was created based on face to face or direct verification using primary ID documents. If local law compliance intended, then local law requirements apply and override. **Entities authorized to verify**: ▪ Authorised internal entity (e.g. human resources dept.) or

	external entity who is legally bound to comply with the verification procedures. ▪ The entity purchasing and managing the e-ID system under contract with WISeKey. If local law compliance intended, then local law requirements apply and override.

12.2.3 Infrastructure Certificates

CP Identifier	Validation Policy
Issuing CA Certificate	See section 12.1
CertifyID URA Admin Certificate	URA Admin Certificates must be issued according to the same rules than a "CertifyID Qualified Personal Certificate", adding an additional validation to ensure that the administrator can only generate the private key in a hardware device (cryptographic USB token or smartcard) which will enforce strong authentication for operations related to certificate generation
CertifyID OCSP Certificate	OCSP Certificates are issued by authorized operators of the Certification Authority systems
CertifyID TSA Certificate	TSA Certificates require a Key Creation Ceremony, audited by an authorized WISeKey representative. The CertifyID TSP regulates this process

13 Annex D: Policy Qualifiers

13.1 Policy Qualifier extension usage

End-entity certificates may include, where appropriate and according to the CA/Browser Forum requirements, the appropriate policy qualifiers. In particular, the policy qualifiers are mandatory for SSL certificates.

As a general rule, the information included in the end-user certificates will be as follows:

	[1]Certificate Policy: [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: *13.1.1.1.1.1* Notice Text=Only for authorized uses. Seulement pour des usages autorises. Solo para usos autorizados. WISeKey SA Copyright (c) 2005 13.1.1.1.1.2 [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.wisekey.com/repository [2]Certificate Policy: Policy Identifier=<CP-OID> (See section 13.2. CP OID Schema)

13.2 CP OID Schema

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

Public Arch:

2.16.756.5.14

<PUBLIC-ARCH>.4 – OISTE WISeKey Global Infrastructure Generation A (SHA-1)

4.1 – Root CP

4.2– Policy CA Class 1 CP (Standard)

4.2.1 – Issuing CA Class 1 CP

4.2.2 – Issuing CA Class 1 CP Extended

4.3– Policy CA Class 2 CP- (Advanced)

4.3.1 – Issuing CA Class 2 CP

4.3.2.1 – Class 2 End Entity CPs

4.3.2.1.1 – CertifyID Advanced Individual Secure Mail

4.3.2.1.2 – CertifyID Advanced Individual Digital Signature

4.3.2.1.3 – CertifyID Advanced Corporate Digital Signature

4.3.2.1.4 – CertifyID Advanced SSL Certificate

4.4– Policy CA Class 3 CP (Qualified)

4.4.1 – Issuing CA Class 3 CP

4.4.2.1 – Class 3 End Entity CPs

4.4.2.1.1 – CertifyID Qualified Individual

4.4.2.1.2 – CertifyID Qualified Corporate

4.4.2.1.3 – CertifyID Qualified Individual for Adobe

4.4.2.1.4 – CertifyID Qualified Corporate for Adobe

4.5– Policy CA Class 4 CP

4.5.1 – Issuing CA Class 4 CP

4.6 – Pilot CP

4.7 – Time Stamping Service

4.7.1. – Time Stamp Policy CP

4.8 – OCSP Service

4.8.1. --- OCSP Policy CP

<PUBLIC-ARCH>.7 – OISTE WISeKey Global Infrastructure Generation B (SHA-256)

7.1 – Root CP

7.2 – Policy CA CP

7.3 – Issuing CA CP

7.4 – End Entity CP

7.4.0 – CertifyID URA Admin Certificate

7.4.1 – CertifyID Personal Standard Certificate

7.4.2 – CertifyID Personal Advanced Certificate

7.4.3 – CertifyID Corporate Advanced Certificate

7.4.4 – CertifyID Personal Qualified Certificate

7.4.5 – CertifyID Corporate Qualified Certificate

7.4.6 – CertifyID Standard SSL Certificate

7.4.7 – CertifyID Advanced OV SSL Certificate

7.4.8 – CertifyID Advanced EV SSL Certificate

7.4.9 – CertifyID Advanced EV Code Signing Certificate [RESERVED]

7.5 – Pilot CP

7.6 – Time Stamp Policy CP

7.7 – OCSP Service