OISTE Foundation

OISTE Global Trust Model

Certificate Policy (CP) for SSL Certificates

Date: 18/7/2024

Version:

Status:

No. Of Pages: 40

OID:

Classification:

File: OGTM - CP SSL Certificates.v1.6.docx

Published by: OISTE Policy Approval Authority

Documentation management

Document Approval

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

Version history

Version	Date	Comments

1.0

25/2/2019

First version

1.1

10/10/2020

Minor change to support DV certificates without Subject contents

1.2

3/2/2021

Include mandate to disclose validation sources

1.3

3/2/2022

Annual review. No changes.

1.4

30/1/2023

Annual review. No changes

1.5

24/1/2024

Annual review. No significant changes

1.6

18/7/2024

Annual review. No significant changes

**
**

Contents

Introductions

Overview

The Certification Policy (CP) documents published by the OISTE Foundation describe the stipulations to be implemented by any Certification Authority, adhered to the OISTE Global Trust Model, in order to issue and manage certificates of a particular type.

This CP document discloses the stipulations related to "SSL Certificates", intended to be issued to, and used by, Software Applications, such web servers, requiring a "Server Authentication" capability. The stipulations of this CP have been defined in compliance of the "Baseline Requirements for SSL Certificates" issued by the CA/Browser Forum, to which all CAs operating under the OISTE Global Trust Model with capability to issue SSL Certificates must commit

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

The OISTE Global Trust Model (**OGTM from now on**) has been designed and are operated in accordance with the broad strategic direction of international PKI (Public Key Infrastructure) standards as well as their application to concrete

identity frameworks in different domains (e.g. ID cards, passports, health cards, Internet of Things) and is intended to serve as a common Trust Model for Certification Authorities worldwide that comply with OISTE requirements.

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

This document is developed per the recommendations found in the document **RFC3647** 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 the CP documents is to disclose the Policies to be adopted in the **OGTM** for the issuance of digital certificates. It is organized in the following sections:

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

The OGTM CP/CPS Documentation Framework

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

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

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

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

Document Name and Identification

Name

OGTM Certificate Policy for SSL Certificates

Version

1.6

OID

2.16.756.5.14.7.1

Issuance date

18/7/2024

Location

This document can be found at /repository

PKI Participants

Certification authorities

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

Registration authorities

As stipulated in the CPS published by the Issuing CA.

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.

Subscribers for certificates issued under this CP are, in perticular, natural and legal persons requiring to protect their internet and communication servers, by means of authentication and encryption.

Relying parties

All persons and entities that trust the certificates issued by certification authorities operating under the **OGTM** Trust Model are considered to be "relying parties" (or trusted third parties). These relying parties do not necessarily need to be a subscriber of an **OGTM** certificate but are requested to accept the "Relying Party agreement ", as disclosed by the Issuing CA in its CPS.

Other participants

As stipulated in the CPS published by the Issuing CA.

Certificate Usage

Appropriate Certificate Uses

CP Identifier

Description

Permitted uses

OISTE Standard DV SSL1 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, Server Authentication

OISTE Advanced OV 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 Forum Baseline Requirements.

Digital Signature, Encryption, Server Authentication

OISTE 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, Server Authentication

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.REF

Prohibited certificate uses

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

Policy Administration

Organization administering the document

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

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

Contact Person (Contact Information)

Name

OISTE Foundation - OGTM Policy Approval Authority

email address

cps@oiste.org

Address

Av. Louis-Casaï, 58 CH-1216 Cointrin - Geneva (Switzerland)

Person determining CPS suitability for the policy

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

CPS approval procedures

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

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

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

Definitions and Acronyms

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

Publication and Repository Responsibilities

This section contains the provisions regarding the publication of policies, certificates and other public information needed for the participants to interoperate with the **OGTM**, in what respects in particular to the certificates issued to Persons. The general stipulations will be published in the appropriate CPS.

Repositories

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

- Policies repository for disclosure of CP, CPS and related information. This repository is a set of web pages and services available at the URL /repository
- Certificate and Certificate Revocation information repositories: *As stipulated in the CPS published by the Issuing CA.*

Publication

As stipulated in the CPS published by the Issuing CA.

Time or frequency of publication

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

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

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

Access control on repositories

As stipulated in the CPS published by the Issuing CA.

Identification and Authentication

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

This document reflects the common practices to be implemented by an Issuing CA authorized to issue SSL Certificates.

If this CP allows multiple practices for a particular section, it must be understood that this CP will stipulate all the allowed practices and that the CPS disclosed by the Subordinate CA can particularize which practices are implemented and the relevant details on the process.

Naming

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

Types of names

All subscribers are assigned a Distinguished Name (DN) according to the X.501 Standard. This DN is optionally 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.

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.

Anonymity of subscribers and pseudonyms

This CP doesn't allow anonymity or pseudonyms in the SSL certificates.

Rules for interpreting various name forms

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

Uniqueness of names

The uniqueness of names for SSL Certificates must be assured by *requiring a combination of domain names, organization name combined/associated with a unique serial integer.*

Recognition, authentication, and role of trademarks

As stipulated in the CPS published by the Issuing CA.

Initial Identity Validation

Issuing CAs implementing this CP must perform the identity validation as stipulated in the following sections.

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 equivalent methods implemented by the Issuing CA.

Authentication of organization identity

The authentication of organization identity for SSL certificates will follow the following rules. **The Issuing CA must detail in its CPS which of the methods are used and how are implemented.**

CP Identifier

Validation Policy

OISTE Standard DV SSL Certificate

The Issuing CA must validate the Applicant's right to use or control each domain name that will be listed in the Subject Alternative Name field of a Certificate by using at least one of the procedures listed in section 3.2.2.4 o the Baseline Requirements.

OISTE Advanced OV SSL Certificate

The Issuing CA must execute the domain validation procedures as required for DV SSL certificates.

Additionally, the Issuing CA must verify:

The identity and address of the Applicant using the procedures found in section 3.2.2.1 and/or section 3.2.3 of the Baseline Requirements.

Any DBA included in a Certificate using a third party or government source, attestation letter, or reliable form of identification in accordance with section 3.2.2 of the Baseline Requirements.

OISTE Advanced EV SSL Certificate

The Issuing CA must execute the domain validation procedures as required for DV and OV SSL certificates.

Additionally, the Issuing CA must do the specific validations mandated by the EV Guidelines issued by the CAB/Forum.

Additionally, the Issuing CA must reference in its CPS the list of validation sources using for these verifications.

Authentication of individual identity

The RA designated by the Issuing CA should obtain from the Applicant a valid Photo-ID issued by a competent government. Further identity proofs can be required if necessary.

In particular for EV SSL certificates, the Issuing CA must endure compliance with the EV Guidelines.

Non-verified subscriber information

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

Validation of authority

The validation of authority for SSL certificates will follow the following rules. **The Issuing CA must detail in its CPS which of the methods are used and how are implemented.**

CP Identifier

Validation Policy

OISTE Standard DV SSL Certificate

The Issuing CA must verify the authority of the requester is verified by using one or more of the procedures listed in section 3.2.2.4. of the Baseline Requirements.

OISTE Advanced OV SSL Certificate

The Issuing CA must verify the authority of the requester is verified by using one or more of the procedures listed in section 3.2.5. of the Baseline Requirements.

OISTE Advanced EV SSL Certificate

The Issuing CA must apply the requirements of section 11.8.3 of the EV Guidelines.

Criteria for interoperation

As stipulated in the CPS published by the Issuing CA.

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).

Identification and authentication for routine re-key

The certificate subscriber can request a routine re-key by authenticating himself with one of these methods:

- Username & Password
- A valid digital certificate linked to the user account

The information of the subscriber must be revalidated periodically, in particular for SSL Certificates the maximum reuse period is as defined by the CAB/Forum (397 days).

Identification and authentication for re-key after revocation

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

Identification and Authentication for Revocation Requests

The Identification Policy for revocation requests is the same as stipulated for routine re-keys.

Certificate Life-Cycle Operational Requirements

The stipulations included in this section are generally disclosed in the CPS published by the Issuing CA, unless otherwise specified in the following subsections.

Certificate Application

As stipulated in the CPS published by the Issuing CA.

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.

Enrolment process and responsibilities

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

Certificate Application Processing

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

Performing identification and authentication functions

The identification and authentication functions can be delegated by the Issuing CA to the Registration Authorities operating under the **OGTM**.

The steps to be executed by the Issuing CA or RA are as follows:

- As a first step, the Issuing CA or RA will perform the verifications stipulated in section 3.2.
- As a second step, the CA must check the DNS for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, according to the procedure in RFC 6844. **The Issuing CA must specify in its CPS the domains that must appear in the CAA records.**
- As a third step, the Issuing CA must check the certificate details against a list of previously revoked Certificates and rejected certificate requests to identify suspicious certificate requests.

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

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 Certificate Policy and the appropriate CPS.

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

Time to process certificate applications

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

Certificate Issuance

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

CA actions during certificate issuance

As stipulated in the CPS published by the Issuing CA.

Notifications to subscriber by the CA of issuance of certificate

As stipulated in the CPS published by the Issuing CA.

Certificate Acceptance

As stipulated in the CPS published by the Issuing CA.

Conduct constituting certificate acceptance

As stipulated in the CPS published by the Issuing CA.

Publication of the certificate by the CA

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

Notification of certificate issuance by the CA to other entities

As stipulated in the CPS published by the Issuing CA.

Key Pair and Certificate Usage

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

Subscriber private key and certificate usage

Any party using these certificates shall use software that is compliant with X.509 and applicable IETF PKIX standards. The Issuer CA can specify restrictions on the use of a Certificate through certificate extensions and shall specify the mechanism(s) to determine certificate validity (CRLs and OCSP).

Relying Parties must process and comply with this information in accordance with their obligations as per the Relaying Party Agreement published by the Issuing CA.

Relying party public key and certificate usage

As stipulated in the CPS published by the Issuing CA.

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.

Circumstance for certificate renewal

For SSL Certificates it is allowed the certificate renewal for the purpose of extending the validity period and always considering the requirements for re-verification periods stipulated in section 3.3 of this CP.

Who may request renewal

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

Processing certificate renewal requests

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

Notification of new certificate issuance to subscriber

As stipulated in the CPS published by the Issuing CA.

Conduct constituting acceptance of a renewal certificate

As stipulated in the CPS published by the Issuing CA.

Publication of the renewal certificate by the CA

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

Notification of certificate issuance by the CA to other entities

As stipulated in the CPS published by the Issuing CA.

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.

Circumstance for certificate re-key

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

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.

Processing certificate re-keying requests

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

Notification of new certificate issuance to subscriber

As stipulated in the CPS published by the Issuing CA.

Conduct constituting acceptance of a re-keyed certificate

As stipulated in the CPS published by the Issuing CA.

Publication of the re-keyed certificate by the CA

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

Notification of certificate issuance by the CA to other entities

As stipulated in the CPS published by the Issuing CA.

Certificate Modification

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

Circumstance for certificate modification

Does not apply.

Who may request certificate modification

Does not apply.

Processing certificate modification requests

Does not apply.

Notification of new certificate issuance to subscriber

Does not apply.

Conduct constituting acceptance of modified certificate

Does not apply.

Publication of the modified certificate by the CA

Does not apply.

Notification of certificate issuance by the CA to other entities

Does not apply.

Certificate Revocation and Suspension

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

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

The stipulations for this section must be disclosed in the CPS, and therefore the reader must refer to that document for more information.

Circumstances for revocation

As stipulated in the CPS published by the Issuing CA.

Who can request revocation

As stipulated in the CPS published by the Issuing CA.

Procedure for revocation request

As stipulated in the CPS published by the Issuing CA.

Revocation request grace period

As stipulated in the CPS published by the Issuing CA.

Time within which CA must process the revocation request

As stipulated in the CPS published by the Issuing CA.

Revocation checking requirement for relying parties

As stipulated in the CPS published by the Issuing CA.

CRL issuance frequency

As stipulated in the CPS published by the Issuing CA.

Maximum latency for CRLs

As stipulated in the CPS published by the Issuing CA.

On-line revocation/status checking availability

As stipulated in the CPS published by the Issuing CA.

On-line revocation checking requirements

As stipulated in the CPS published by the Issuing CA.

Other forms of revocation advertisements available

No stipulations.

Special requirements regarding key compromise

As stipulated in the CPS published by the Issuing CA.

Circumstances for suspension

Suspension is not permitted for SSL Certificates.

Who can request suspension

Does not apply.

Procedure for suspension request

Does not apply.

Limits on suspension period

Does not apply.

Certificate Status Services

For SSL Certificates, the Issuing CA must provide certificate status validation services, by means of Certificate Revocation Lists and OCSP responder. The details of such services must be detailed in the CPS published by the Issuing CA.

Operational characteristics

As stipulated in the CPS published by the Issuing CA.

Service availability

As stipulated in the CPS published by the Issuing CA.

Optional features

No stipulation.

End of Subscription

As stipulated in the CPS published by the Issuing CA.

Key Escrow and Recovery

Key escrow is not permitted for SSL Certificates.

Key escrow and recovery policy and practices

Does not apply.

Session key encapsulation and recovery policy and practices

Does not apply.

Management, Operational, and Physical Controls

As stipulated in the CPS published by the Issuing CA.

Physical Security Controls

As stipulated in the CPS published by the Issuing CA.

Site location and construction

As stipulated in the CPS published by the Issuing CA.

Physical access

As stipulated in the CPS published by the Issuing CA.

Power and air conditioning

As stipulated in the CPS published by the Issuing CA.

Water exposures

As stipulated in the CPS published by the Issuing CA.

Fire prevention and protection

As stipulated in the CPS published by the Issuing CA.

Media storage

As stipulated in the CPS published by the Issuing CA.

Waste disposal

As stipulated in the CPS published by the Issuing CA.

Backup

As stipulated in the CPS published by the Issuing CA.

Procedural Controls

As stipulated in the CPS published by the Issuing CA.

Trusted roles

As stipulated in the CPS published by the Issuing CA.

Number of persons required per task

As stipulated in the CPS published by the Issuing CA.

Identification and authentication for each role

As stipulated in the CPS published by the Issuing CA.

Roles requiring separation of duties

As stipulated in the CPS published by the Issuing CA.

Personnel Security Controls

As stipulated in the CPS published by the Issuing CA.

Qualifications, experience, and clearance requirements

As stipulated in the CPS published by the Issuing CA.

Background check procedures

As stipulated in the CPS published by the Issuing CA.

Training requirements

As stipulated in the CPS published by the Issuing CA.

Retraining frequency and requirements

As stipulated in the CPS published by the Issuing CA.

Job rotation frequency and sequence

As stipulated in the CPS published by the Issuing CA.

Sanctions for unauthorized actions

As stipulated in the CPS published by the Issuing CA.

Independent contractor requirements

As stipulated in the CPS published by the Issuing CA.

Documentation supplied to personnel

As stipulated in the CPS published by the Issuing CA.

Contract termination and assigned role change procedures

As stipulated in the CPS published by the Issuing CA.

Audit Logging Procedures

As stipulated in the CPS published by the Issuing CA.

Types of events recorded

As stipulated in the CPS published by the Issuing CA.

Frequency of processing log

As stipulated in the CPS published by the Issuing CA.

Retention period for audit log

As stipulated in the CPS published by the Issuing CA.

Protection of audit log

As stipulated in the CPS published by the Issuing CA.

Audit log backup procedures

As stipulated in the CPS published by the Issuing CA.

Audit collection system (internal vs. external)

As stipulated in the CPS published by the Issuing CA.

Notification to event-causing subject

As stipulated in the CPS published by the Issuing CA.

Vulnerability assessments

As stipulated in the CPS published by the Issuing CA.

Records Archival

As stipulated in the CPS published by the Issuing CA.

Types of records archived

As stipulated in the CPS published by the Issuing CA.

Retention period for archive

As stipulated in the CPS published by the Issuing CA.

Protection of archive

As stipulated in the CPS published by the Issuing CA.

Archive backup procedures

As stipulated in the CPS published by the Issuing CA.

Requirements for time-stamping of records

As stipulated in the CPS published by the Issuing CA.

Archive collection system (internal or external)

As stipulated in the CPS published by the Issuing CA.

Procedures to obtain and verify archive information

As stipulated in the CPS published by the Issuing CA.

Key Changeover

As stipulated in the CPS published by the Issuing CA.

Compromise and Disaster Recovery

As stipulated in the CPS published by the Issuing CA.

Incident and compromise handling procedures

As stipulated in the CPS published by the Issuing CA.

Computing resources, software, and/or data are corrupted

As stipulated in the CPS published by the Issuing CA.

Entity private key compromise procedures

As stipulated in the CPS published by the Issuing CA.

Business continuity capabilities after a disaster

As stipulated in the CPS published by the Issuing CA.

CA or RA Termination

As stipulated in the CPS published by the Issuing CA.

Technical Security Controls

Most of the stipulations of this section will refer to the CPS published by the Issuing CA. In the following sections only particular policies for SSL Certificates are stipulated, when appropriate.

Key Pair Generation and Installation

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

Key pair generation

Key Pairs for SSL Certificates can be generated by software components, except the "OISTE Qualified Personal/Corporate Certificates", which must be generated in Secure Signature Hardware Devices (FIPS 140-1 Level 2 and equivalents, or higher).

Subscribers who generate their own keys shall use a FIPS-approved method and either a validated hardware or validated software cryptographic module, depending on the level of assurance desired.

Private key delivery to subscriber

As stipulated in the CPS published by the Issuing CA.

Public key delivery to certificate issuer

As stipulated in the CPS published by the Issuing CA.

CA public key delivery to relying parties

As stipulated in the CPS published by the Issuing CA.

Key sizes

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

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

Public key parameters generation and quality checking

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

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

SSL Certificates assert key usages based on the intended application of the Key Pair. In particular, Certificates to be used for digital signatures (including authentication) set the digitalSignature and keyEncipherment bits.

Private Key Protection and Cryptographic Module Engineering Controls

The Issuing CA must establish controls to ensure that the risks derived from a private key compromise are managed and kept under reasonable levels.

Cryptographic module standards and controls

Requirements for End-User cryptographic devices (if any) can vary in terms of the expected assurance level, as indicated in section 6.1.1.

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

As stipulated in the CPS published by the Issuing CA.

Private key escrow

As stipulated in section 4.12 of this CP and in the CPS published by the Issuing CA.

Private key backup

Backup for SSL Certificates is considered equivalent of escrow and not permitted, as stipulated in section 4.12 of this CP and in the CPS published by the Issuing CA.

Private key archival

The CA shall not provide key archival services.

Private key transfer into or from a cryptographic module

No stipulation

Private key storage on cryptographic module

No stipulation additional to the requirements expressed in section 6.1.

Method of activating private key

As stipulated in the CPS published by the Issuing CA.

Method of deactivating private key

As stipulated in the CPS published by the Issuing CA.

Method of destroying private key

As stipulated in the CPS published by the Issuing CA.

Cryptographic Module Rating

No stipulation additional to section 6.2.1.

Other Aspects of Key Pair Management

This section includes additional stipulations regarding key pair management.

Public key archival

As stipulated in the CPS published by the Issuing CA.

Certificate operational periods and key pair usage periods

For SSL Certificates, the Certificate operational period is equivalent to the key pair usage period and limited to 397 days.

Activation Data

As stipulated in the CPS published by the Issuing CA.

Activation data generation and installation

As stipulated in the CPS published by the Issuing CA.

Activation data protection

As stipulated in the CPS published by the Issuing CA.

Other aspects of activation data

No stipulation.

Computer Security Controls

As stipulated in the CPS published by the Issuing CA.

Specific computer security technical requirements

As stipulated in the CPS published by the Issuing CA.

Computer security rating

As stipulated in the CPS published by the Issuing CA.

Life Cycle Security Controls

As stipulated in the CPS published by the Issuing CA.

System development controls

As stipulated in the CPS published by the Issuing CA.

Security management controls

As stipulated in the CPS published by the Issuing CA.

Life cycle security controls

As stipulated in the CPS published by the Issuing CA.

Network Security Controls

As stipulated in the CPS published by the Issuing CA.

Time-stamping

As stipulated in the CPS published by the Issuing CA.

Certificate and CRL Profiles

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

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

Certificate Profile

This section refers to the certificate profiles of SSL Certificates issued under the OISTE Trust Model.

Version number(s)

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

Certificate extensions

The different extension profiles for SSL Certificates are listed below. This information is included as basic reference. Issuing CAs must conform to the allowed certificate profiles mandated by the CAB/F Baseline Requirements.

OISTE Standard DV SSL Certificate 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 section 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 values: Digital Signature, Key Encipherment (a0)

Extended Key Usage

Client Authentication, Server Authentication

SubjectAltName

<List of SAN> (at least one)

OISTE Advanced OV SSL Certificate 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 Section 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. Allowed Values: Data Encipherment, Digital Signature, Key Encipherment

Extended Key Usage

Client Authentication, Server Authentication

SubjectAltName

<List of SAN> (at least one)

OISTE Advanced EV SSL Certificate 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 Section 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. Allowed Values: Data Encipherment, Digital Signature, Key Encipherment

Extended Key Usage

Client Authentication, Server Authentication

SubjectAltName

<List of SAN> (at least one)

Algorithm object identifiers

The allowed Algorithm object identifiers are:

- **sha256withRSAEncryption**:
  OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- **ecdsa-with-SHA256**
  OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(10045) pkcs(4) pkcs-1(3) 2}

- **ecdsa-with-SHA256**
  OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(10045) pkcs(4) pkcs-1(3) 3}

Name forms

Certificates issued under the **OGTM** contain the "Distinguished Name", in X.500 format, for the issuer and the subscriber, set in the fields "Issuer Name" and "Subject Name" respectively.

Name constraints

No stipulation for subscriber certificates.

Certificate policy object identifier

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

In particular for this CP, the following OID can be used:

<Public Arch> = 2.16.756.5.14

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

4.3.2.1.4 – OISTE Advanced SSL Certificate

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

7.4.6 – OISTE Standard SSL Certificate

7.4.7 – OISTE Advanced OV SSL Certificate

7.4.8 – OISTE Advanced EV SSL Certificate

CAB/Forum Policy qualifiers for SSL Certificates (can be added to or can substitute the OISTE OIDs when used in Publicly-Trusted certificates)

2.23.140.1.2.1 – OISTE Standard SSL Certificate

2.23.140.1.2.2 – OISTE OV SSL Certificate

2.23.140.1.1 – OISTE EV SSL Certificate

Usage of Policy Constraints extension

No stipulation for subscriber certificates. The CA can disclose additional stipulations in its CPS for CA certificates.

Policy qualifiers syntax and semantics

No stipulation for subscriber certificates. The CA can disclose additional stipulations in its CPS for CA certificates.

Processing semantics for the critical Certificate Policies extension

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

CRL Profile

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

Version number(s)

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

CRL Profile and CRL entry extensions

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

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

OCSP Profile

Issuing CAs can optionally provide OCSP services for particular types of SSL Certificates.

Version number(s)

OGTM provides OCSP responses in accordance with industry standards.

OCSP extensions

No stipulation.

Compliance Audit and Other Assessment

This section is included in this CP document only for standardization purposes. The reader must refer to the CPS published by the Issuing CA for all the relevant stipulations.

Frequency or circumstances of assessment

As stipulated in the CPS published by the Issuing CA.

Identity/qualifications of assessor

As stipulated in the CPS published by the Issuing CA.

Assessor's relationship to assessed entity

As stipulated in the CPS published by the Issuing CA.

Topics covered by assessment

As stipulated in the CPS published by the Issuing CA.

Actions taken as a result of deficiency

As stipulated in the CPS published by the Issuing CA.

Communication of results

As stipulated in the CPS published by the Issuing CA.

Other Business and Legal Matters

This section is included in this CP document only for standardization purposes. The reader must refer to the CPS published by the Issuing CA for all the relevant stipulations.

Fees

As stipulated in the CPS published by the Issuing CA.

Certificate issuance or renewal fees

As stipulated in the CPS published by the Issuing CA.

Certificate access fees

As stipulated in the CPS published by the Issuing CA.

Revocation or status information access fees

As stipulated in the CPS published by the Issuing CA.

Fees for other services

As stipulated in the CPS published by the Issuing CA.

Refund policy

As stipulated in the CPS published by the Issuing CA.

Financial Responsibility

As stipulated in the CPS published by the Issuing CA.

Insurance coverage

As stipulated in the CPS published by the Issuing CA.

Other assets

As stipulated in the CPS published by the Issuing CA.

Insurance or warranty coverage for end-entities

As stipulated in the CPS published by the Issuing CA.

Confidentiality of Business Information

As stipulated in the CPS published by the Issuing CA.

Scope of confidential information

As stipulated in the CPS published by the Issuing CA.

Information not within the scope of confidential information

As stipulated in the CPS published by the Issuing CA.

Responsibility to protect confidential information

As stipulated in the CPS published by the Issuing CA.

Privacy of Personal Information

As stipulated in the CPS published by the Issuing CA.

Privacy plan

As stipulated in the CPS published by the subordinate CA.

Information treated as private

As stipulated in the CPS published by the Issuing CA.

Information not deemed private

As stipulated in the CPS published by the Issuing CA.

Responsibility to protect private information

As stipulated in the CPS published by the Issuing CA.

Notice and consent to use private information

As stipulated in the CPS published by the Issuing CA.

Disclosure pursuant to judicial or administrative process

As stipulated in the CPS published by the Issuing CA.

Other information disclosure circumstances

As stipulated in the CPS published by the Issuing CA.

Intellectual Property Rights

As stipulated in the CPS published by the Issuing CA.

Representations and Warranties

As stipulated in the CPS published by the Issuing CA.

CA representations and warranties

As stipulated in the CPS published by the Issuing CA.

RA representations and warranties

As stipulated in the CPS published by the Issuing CA.

Subscriber representations and warranties

As stipulated in the CPS published by the Issuing CA.

Relying party representations and warranties

As stipulated in the CPS published by the Issuing CA.

Representations and warranties of other participants

As stipulated in the CPS published by the Issuing CA.

Disclaimers of Warranties

As stipulated in the CPS published by the Issuing CA.

Limitations of Liability

As stipulated in the CPS published by the Issuing CA.

Indemnities

As stipulated in the CPS published by the Issuing CA.

Term and Termination

As stipulated in the CPS published by the Issuing CA.

Term

As stipulated in the CPS published by the Issuing CA.

Termination

As stipulated in the CPS published by the Issuing CA.

Effect of termination and survival

As stipulated in the CPS published by the Issuing CA.

Individual notices and communications with participants

As stipulated in the CPS published by the Issuing CA.

Amendments

As stipulated in the CPS published by the Issuing CA.

Procedure for amendment

As stipulated in the CPS published by the Issuing CA.

Notification mechanism and period

As stipulated in the CPS published by the Issuing CA.

Circumstances under which OID must be changed

As stipulated in the CPS published by the Issuing CA.

Dispute Resolution Procedures

As stipulated in the CPS published by the Issuing CA.

Governing Law

As stipulated in the CPS published by the Issuing CA.

Compliance with Applicable Law

As stipulated in the CPS published by the Issuing CA.

Miscellaneous Provisions

As stipulated in the CPS published by the Issuing CA.

Entire agreement

As stipulated in the CPS published by the Issuing CA.

Assignment

As stipulated in the CPS published by the Issuing CA.

Severability

As stipulated in the CPS published by the Issuing CA.

Enforcement (attorneys' fees and waiver of rights)

As stipulated in the CPS published by the Issuing CA.

Force Majeure

As stipulated in the CPS published by the Issuing CA.

Other Provisions

As stipulated in the CPS published by the Issuing CA.

Annex A: Glossary

AATL Adobe Approved Trust List

CA Certificate Authority or Certification Authority

CAA Certification Authority Authorization

CAB "CA/Browser" as in "CAB Forum"

CMS Card Management System

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

CSR Certificate Signing Request

CT Certificate Transparency

DBA Doing Business As (also known as "Trading As")

DV Domain Validated

ETSI European Telecommunications Standards Institute

EU European Union

EV Extended Validation

FIPS (US Government) Federal Information Processing Standard FQDN Fully Qualified Domain Name

FTP File Transfer Protocol

HISP Health Information Service Provider

HSM Hardware Security Module

HTTP Hypertext Transfer Protocol

IANA Internet Assigned Numbers Authority

ICANN Internet Corporation for Assigned Names and Numbers IdM Identity Management System

IDN Internationalized Domain Name

ISSO Information System Security Officer (also CSO, Chief Security Officer)

IETF Internet Engineering Task Force

IGTF International Grid Trust Federation

ITU International Telecommunication Union

IV Individual Validated

MICS Member-Integrated Credential Service (IGTF) NIST National Institute of Standards and Technology OCSP Online Certificate Status Protocol

OID Object Identifier

OV Organization Validated

PAA Policy Approval Authority

PIN Personal Identification Number (e.g. a secret access code)

PKI Public Key Infrastructure

PKIX IETF Working Group on Public Key Infrastructure

RA Registration Authority

RFC Request for Comments (at IETF.org)

SAN Subject Alternative Name

SHA Secure Hashing Algorithm

SSL Secure Sockets Layer

TLD Top-Level Domain

TLS Transport Layer Security

TSA Time Stamping Authority

TST Time-Stamp Token

TTL Time To Live

UTC Coordinated Universal Time

X.509 The ITU-T standard for Certificates and their corresponding authentication framework