OISTE Global Trust Model

Certificate Policy (CP) for SSL Certificates

Date: 30/1/2023  
Version: 1.4

Status: FINAL  
No. Of Pages: 40

OID: 2.16.756.5.14.7.4  
Classification: PUBLIC

File: OGTM - CP SSL Certificates.v1.4.docx

Published by: OISTE Policy Approval Authority

This document is issued by the OISTE Foundation, and licensed under a Creative Commons Attribution-NoDerivatives 4.0 (CC BY-ND 4.0)
Documentation management

Document Approval

<table>
<thead>
<tr>
<th>Version</th>
<th>PAA Representative #1</th>
<th>PAA Representative #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.4</td>
<td>Name:</td>
<td>Name:</td>
</tr>
<tr>
<td></td>
<td>Signature:</td>
<td>Signature:</td>
</tr>
</tbody>
</table>

Version history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>25/2/2019</td>
<td>First version</td>
</tr>
<tr>
<td>1.1</td>
<td>10/10/2020</td>
<td>Minor change to support DV certificates without Subject contents</td>
</tr>
<tr>
<td>1.2</td>
<td>3/2/2021</td>
<td>Include mandate to disclose validation sources</td>
</tr>
<tr>
<td>1.3</td>
<td>3/2/2022</td>
<td>Annual review. No changes.</td>
</tr>
<tr>
<td>1.4</td>
<td>30/1/2023</td>
<td>Annual review. No changes.</td>
</tr>
</tbody>
</table>
OGTM – Certificate Policy (CP) for SSL Certificates

Contents

1 Introductions .......................................................................................................................... 9

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

1.2 Document Name and Identification .................................................................................... 10

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

1.4 Certificate Usage ............................................................................................................. 11
1.4.1 Appropriate Certificate Uses ....................................................................................... 11
1.4.2 Prohibited certificate uses ......................................................................................... 12

1.5 Policy Administration ....................................................................................................... 12
1.5.1 Organization administering the document .................................................................... 12
1.5.2 Contact Person (Contact Information) ........................................................................ 13
1.5.3 Person determining CPS suitability for the policy ....................................................... 13
1.5.4 CPS approval procedures ............................................................................................ 13

1.6 Definitions and Acronyms ............................................................................................... 13

2 Publication and Repository Responsibilities ......................................................................... 14

2.1 Repositories ..................................................................................................................... 14

2.2 Publication ....................................................................................................................... 14

2.3 Time or frequency of publication .................................................................................... 14

2.4 Access control on repositories ......................................................................................... 14

3 Identification and Authentication ......................................................................................... 15

3.1 Naming ............................................................................................................................. 15
3.1.1 Types of names ............................................................................................................ 15
3.1.2 Need for names to be meaningful .............................................................................. 15
3.1.3 Anonymity of subscribers and pseudonyms .............................................................. 15
3.1.4 Rules for interpreting various name forms ................................................................. 15
3.1.5 Uniqueness of names .................................................................................................. 15
3.1.6 Recognition, authentication, and role of trademarks .................................................. 15

3.2 Initial Identity Validation .................................................................................................. 15
3.2.1 Method to prove possession of private key ................................................................. 16
3.2.2 Authentication of organization identity ...................................................................... 16
3.2.3 Authentication of individual identity ........................................................................... 16
3.2.4 Non-verified subscriber information ........................................................................... 16
3.2.5 Validation of authority ................................................................................................. 17
3.2.6 Criteria for interoperation ......................................................................................... 17

3.3 Identification and Authentication for Re-key Requests .................................................... 17
3.3.1 Identification and authentication for routine re-key ..................................................... 17
3.3.2 Identification and authentication for re-key after revocation ..................................... 17

3.4 Identification and Authentication for Revocation Requests ........................................... 17
4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

4.1.2 Enrolment process and responsibilities

4.2 Certificate Application Processing

4.2.1 Performing identification and authentication functions

4.2.2 Approval or rejection of certificate applications

4.2.3 Time to process certificate applications

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

4.3.2 Notifications to subscriber by the CA of issuance of certificate

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

4.4.2 Publication of the certificate by the CA

4.4.3 Notification of issuance of certificate issuance by the CA to other entities

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

4.5.2 Relying party public key and certificate usage

4.6 Certificate Renewal

4.6.1 Circumstance for certificate renewal

4.6.2 Who may request renewal

4.6.3 Processing certificate renewal requests

4.6.4 Notification of new certificate issuance to subscriber

4.6.5 Conduct constituting acceptance of a renewal certificate

4.6.6 Publication of the renewal certificate by the CA

4.6.7 Notification of certificate issuance by the CA to other entities

4.7 Certificate Re-key

4.7.1 Circumstance for certificate re-key

4.7.2 Who may request certification of a new public key

4.7.3 Processing certificate re-keying requests

4.7.4 Notification of new certificate issuance to subscriber

4.7.5 Conduct constituting acceptance of a re-keyed certificate

4.7.6 Publication of the re-keyed certificate by the CA

4.7.7 Notification of certificate issuance by the CA to other entities

4.8 Certificate Modification

4.8.1 Circumstance for certificate modification

4.8.2 Who may request certificate modification

4.8.3 Processing certificate modification requests

4.8.4 Notification of new certificate issuance to subscriber

4.8.5 Conduct constituting acceptance of modified certificate

4.8.6 Publication of the modified certificate by the CA

4.8.7 Notification of certificate issuance by the CA to other entities

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

4.9.2 Who can request revocation

4.9.3 Procedure for revocation request

4.9.4 Revocation request grace period

4.9.5 Time within which CA must process the revocation request

4.9.6 Revocation checking requirement for relying parties

4.9.7 CRL issuance frequency

4.9.8 Maximum latency for CRLs
4.10 Certificate Status Services ........................................................................ 23
  4.10.1 Operational characteristics ...................................................................... 23
  4.10.2 Service availability ................................................................................... 23
  4.10.3 Optional features ..................................................................................... 23

4.11 End of Subscription ...................................................................................... 23

4.12 Key Escrow and Recovery .......................................................................... 23
  4.12.1 Key escrow and recovery policy and practices ........................................ 23
  4.12.2 Session key encapsulation and recovery policy and practices ................ 23

5 Management, Operational, and Physical Controls ....................................... 24

5.1 Physical Security Controls .......................................................................... 24
  5.1.1 Site location and construction ................................................................... 24
  5.1.2 Physical access .......................................................................................... 24
  5.1.3 Power and air conditioning ...................................................................... 24
  5.1.4 Water exposures ....................................................................................... 24
  5.1.5 Fire prevention and protection .................................................................. 24
  5.1.6 Media storage ............................................................................................ 24
  5.1.7 Waste disposal .......................................................................................... 24
  5.1.8 Backup ....................................................................................................... 24

5.2 Procedural Controls ...................................................................................... 24
  5.2.1 Trusted roles ............................................................................................. 24
  5.2.2 Number of persons required per task ......................................................... 24
  5.2.3 Identification and authentication for each role ........................................ 24
  5.2.4 Roles requiring separation of duties .......................................................... 25

5.3 Personnel Security Controls ....................................................................... 25
  5.3.1 Qualifications, experience, and clearance requirements ......................... 25
  5.3.2 Background check procedures .................................................................. 25
  5.3.3 Training requirements .............................................................................. 25
  5.3.4 Retraining frequency and requirements .................................................... 25
  5.3.5 Job rotation frequency and sequence ...................................................... 25
  5.3.6 Sanctions for unauthorized actions ............................................................ 25
  5.3.7 Independent contractor requirements ....................................................... 25
  5.3.8 Documentation supplied to personnel ....................................................... 25
  5.3.9 Contract termination and assigned role change procedures .................... 25

5.4 Audit Logging Procedures .......................................................................... 25
  5.4.1 Types of events recorded .......................................................................... 25
  5.4.2 Frequency of processing log ...................................................................... 25
  5.4.3 Retention period for audit log .................................................................... 26
  5.4.4 Protection of audit log .............................................................................. 26
  5.4.5 Audit log backup procedures ..................................................................... 26
  5.4.6 Audit collection system (internal vs. external) .......................................... 26
  5.4.7 Notification to event-causing subject ......................................................... 26
  5.4.8 Vulnerability assessments ........................................................................ 26

5.5 Records Archival .......................................................................................... 26
5.6 Key Changeover ........................................................................................................ 27

5.7 Compromise and Disaster Recovery ........................................................................ 27
  5.7.1 Incident and compromise handling procedures ....................................................... 27
  5.7.2 Computing resources, software, and/or data are corrupted .................................... 27
  5.7.3 Entity private key compromise procedures ............................................................ 27
  5.7.4 Business continuity capabilities after a disaster ...................................................... 27

5.8 CA or RA Termination .............................................................................................. 27

6 Technical Security Controls ....................................................................................... 28

6.1 Key Pair Generation and Installation ........................................................................ 28
  6.1.1 Key pair generation .............................................................................................. 28
  6.1.2 Private key delivery to subscriber ........................................................................ 28
  6.1.3 Public key delivery to certificate issuer ................................................................. 28
  6.1.4 CA public key delivery to relying parties .............................................................. 28
  6.1.5 Key sizes ............................................................................................................ 28
  6.1.6 Public key parameters generation and quality checking ....................................... 28
  6.1.7 Key usage purposes (as per X.509 v3 key usage field) .......................................... 28

6.2 Private Key Protection and Cryptographic Module Engineering Controls ................ 28
  6.2.1 Cryptographic module standards and controls ...................................................... 29
  6.2.2 Private key (n out of m) multi-person control ....................................................... 29
  6.2.3 Private key escrow .............................................................................................. 29
  6.2.4 Private key backup .............................................................................................. 29
  6.2.5 Private key archival ............................................................................................. 29
  6.2.6 Private key transfer into or from a cryptographic module ..................................... 29
  6.2.7 Private key storage on cryptographic module ....................................................... 29
  6.2.8 Method of activating private key ......................................................................... 29
  6.2.9 Method of deactivating private key ..................................................................... 29
  6.2.10 Method of destroying private key ....................................................................... 29
  6.2.11 Cryptographic Module Rating ........................................................................... 29

6.3 Other Aspects of Key Pair Management .................................................................. 29
  6.3.1 Public key archival .............................................................................................. 29
  6.3.2 Certificate operational periods and key pair usage periods ................................... 29

6.4 Activation Data ....................................................................................................... 30
  6.4.1 Activation data generation and installation ............................................................. 30
  6.4.2 Activation data protection .................................................................................... 30
  6.4.3 Other aspects of activation data ............................................................................ 30

6.5 Computer Security Controls ................................................................................... 30
  6.5.1 Specific computer security technical requirements ................................................ 30
  6.5.2 Computer security rating .................................................................................... 30

6.6 Life Cycle Security Controls ................................................................................... 30
  6.6.1 System development controls ............................................................................. 30
  6.6.2 Security management controls ............................................................................ 30
  6.6.3 Life cycle security controls ................................................................................ 30

6.7 Network Security Controls ..................................................................................... 30
OGTM – Certificate Policy (CP) for SSL Certificates

6.8 Time-stamping ............................................................................................................ 30

7 Certificate and CRL Profiles ......................................................................................... 31

7.1 Certificate Profile ....................................................................................................... 31
7.1.1 Version number(s) ................................................................................................. 31
7.1.2 Certificate extensions ............................................................................................ 31
7.1.3 Algorithm object identifiers .................................................................................. 33
7.1.4 Name forms ............................................................................................................ 33
7.1.5 Name constraints ................................................................................................... 33
7.1.6 Certificate policy object identifier ......................................................................... 33
7.1.7 Usage of Policy Constraints extension ................................................................. 33
7.1.8 Policy qualifiers syntax and semantics ................................................................. 34
7.1.9 Processing semantics for the critical Certificate Policies extension ..................... 34

7.2 CRL Profile .................................................................................................................. 34
7.2.1 Version number(s) ................................................................................................. 34
7.2.2 CRL Profile and CRL entry extensions ................................................................. 34

7.3 OCSP Profile .............................................................................................................. 34
7.3.1 Version number(s) ................................................................................................. 34
7.3.2 OCSP extensions ................................................................................................... 34

8 Compliance Audit and Other Assessment ....................................................................... 35

8.1 Frequency or circumstances of assessment ............................................................... 35
8.2 Identity/qualifications of assessor ............................................................................... 35
8.3 Assessor's relationship to assessed entity .................................................................... 35
8.4 Topics covered by assessment .................................................................................... 35
8.5 Actions taken as a result of deficiency ........................................................................ 35
8.6 Communication of results .......................................................................................... 35

9 Other Business and Legal Matters ................................................................................. 36

9.1 Fees ............................................................................................................................ 36
9.1.1 Certificate issuance or renewal fees ....................................................................... 36
9.1.2 Certificate access fees .......................................................................................... 36
9.1.3 Revocation or status information access fees ...................................................... 36
9.1.4 Fees for other services .......................................................................................... 36
9.1.5 Refund policy ........................................................................................................ 36

9.2 Financial Responsibility ............................................................................................ 36
9.2.1 Insurance coverage .............................................................................................. 36
9.2.2 Other assets .......................................................................................................... 36
9.2.3 Insurance or warranty coverage for end-entities .................................................. 36

9.3 Confidentiality of Business Information ..................................................................... 36
9.3.1 Scope of confidential information ......................................................................... 36
9.3.2 Information not within the scope of confidential information ............................. 36
9.3.3 Responsibility to protect confidential information ................................................ 37

9.4 Privacy of Personal Information .............................................................................. 37
9.4.1 Privacy plan .......................................................................................................... 37
9.4.2 Information treated as private .............................................................................. 37
9.4.3 Information not deemed private .......................................................................... 37
9.4.4 Responsibility to protect private information ....................................................... 37
9.4.5 Notice and consent to use private information .................................................... 37
9.5 Intellectual Property Rights .................................................................................. 37
9.6 Representations and Warranties ......................................................................... 37
  9.6.1 CA representations and warranties .................................................................. 37
  9.6.2 RA representations and warranties .................................................................. 37
  9.6.3 Subscriber representations and warranties ...................................................... 37
  9.6.4 Relying party representations and warranties .................................................. 38
  9.6.5 Representations and warranties of other participants ....................................... 38
9.7 Disclaimers of Warranties ................................................................................... 38
9.8 Limitations of Liability ......................................................................................... 38
9.9 Indemnities ........................................................................................................... 38
9.10 Term and Termination ......................................................................................... 38
   9.10.1 Term ........................................................................................................... 38
   9.10.2 Termination .................................................................................................. 38
   9.10.3 Effect of termination and survival ................................................................. 38
9.11 Individual notices and communications with participants .................................. 38
9.12 Amendments ........................................................................................................ 38
   9.12.1 Procedure for amendment ........................................................................... 38
   9.12.2 Notification mechanism and period ............................................................... 38
   9.12.3 Circumstances under which OID must be changed ...................................... 38
9.13 Dispute Resolution Procedures .......................................................................... 39
9.14 Governing Law ..................................................................................................... 39
9.15 Compliance with Applicable Law ........................................................................ 39
9.16 Miscellaneous Provisions ................................................................................... 39
   9.16.1 Entire agreement .......................................................................................... 39
   9.16.2 Assignment .................................................................................................. 39
   9.16.3 Severability .................................................................................................. 39
   9.16.4 Enforcement (attorneys’ fees and waiver of rights) ....................................... 39
   9.16.5 Force Majeure .............................................................................................. 39
9.17 Other Provisions .................................................................................................. 39
10 Annex A: Glossary ................................................................................................ 40
1 Introductions

1.1 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.

1.1.1 The OGTM CP/CPS Documentation Framework
The main information disclosed by the OGTM in order to expose its practices and policies in the issuance and usages of digital certificates are:

- The Certification Practices Statement (CPS) – The CPS is a statement of the practices that every Certification Authority operating under the OGTM Trust Model employs in issuing, managing, revoking, and renewing or re-keying certificates. This CPS document discloses the stipulations related to the issuance of Subordinate CA Certificates, assigned to entities acting as “Issuing Certification Authorities” under the OGTM. Those entities must publish their own CPS to disclose the stipulations related to end-entity certification practices. **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”.

1.2 Document Name and Identification

<table>
<thead>
<tr>
<th>Name</th>
<th>OGT.M Certificate Policy for SSL Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.4</td>
</tr>
<tr>
<td>OID</td>
<td>2.16.756.5.14.7.1</td>
</tr>
<tr>
<td>Issuance date</td>
<td>30/1/2023</td>
</tr>
<tr>
<td>Location</td>
<td>This document can be found at <a href="http://www.oiste.org/repository">http://www.oiste.org/repository</a></td>
</tr>
</tbody>
</table>
1.3 PKI Participants

1.3.1 Certification authorities

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

1.3.2 Registration authorities

As stipulated in the CPS published by the Issuing CA.

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.

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

1.3.4 Relying parties

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

1.3.5 Other participants

As stipulated in the CPS published by the Issuing CA.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

<table>
<thead>
<tr>
<th>CP Identifier</th>
<th>Description</th>
<th>Permitted uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>OISTE Standard DV SSL Certificate</td>
<td>Medium assurance SSL/TLS certificate. All identification attributes in the certificate are verified. The control</td>
<td>Digital Signature, Encryption, Server Authentication</td>
</tr>
</tbody>
</table>

1 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.
1.4.2 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.

1.5 Policy Administration

1.5.1 Organization administering the document

This document is administered by the **OGTM Policy Approval Authority** (referred from now as **PAA**). The **PAA** has a series of distinct functions but does not operate as a separate legal entity. It is managed and organized in accordance with a process that draws on expertise within the **OISTE Foundation**. The **PAA** has been established to develop, review and/or approve the practices, policies and procedures for the entire Trust Model, subject to guidelines established by the members and advisors of the **OISTE Foundation**.
1.5.2 Contact Person (Contact Information)

<table>
<thead>
<tr>
<th>Name</th>
<th>OISTE Foundation - OGTM Policy Approval Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>email address</td>
<td><a href="mailto:cps@oiste.org">cps@oiste.org</a></td>
</tr>
<tr>
<td>Address</td>
<td>Av. Louis-Casai, 58 CH-1216 Cointrin - Geneva (Switzerland)</td>
</tr>
</tbody>
</table>

1.5.3 Person determining CPS suitability for the policy

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

1.5.4 CPS approval procedures

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

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

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

1.6 Definitions and Acronyms

Definitions and Acronyms are included in Annex A (Glossary).
2 Publication and Repository Responsibilities

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

2.1 Repositories

The main repositories of the OGTM are:

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

2.2 Publication

As stipulated in the CPS published by the Issuing CA.

2.3 Time or frequency of publication

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

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

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

2.4 Access control on repositories

As stipulated in the CPS published by the Issuing CA.
3 Identification and Authentication

The OGTM mandates the fulfillment of a set of required minimum controls that ensure the authenticity of the data included in certificates. These controls are enforced during the full lifecycle of certificates, certificate requests, and related documents. 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.

3.1 Naming

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

3.1.1 Types of names

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

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

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

3.1.4 Rules for interpreting various name forms

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

3.1.5 Uniqueness of names

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.

3.1.6 Recognition, authentication, and role of trademarks

As stipulated in the CPS published by the Issuing CA.

3.2 Initial Identity Validation

Issuing CAs implementing this CP must perform the identity validation as stipulated in the following sections.
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 equivalent methods implemented by the Issuing CA.

3.2.2 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.

<table>
<thead>
<tr>
<th>CP Identifier</th>
<th>Validation Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>OISTE Standard DV SSL Certificate</td>
<td>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 of the Baseline Requirements.</td>
</tr>
</tbody>
</table>
| 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.

3.2.3 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.

3.2.4 Non-verified subscriber information

OGTM doesn’t allow to include non-verified identity-related information in any certificate issued by a certification authority operating in the trust model.
3.2.5 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.

<table>
<thead>
<tr>
<th>CP Identifier</th>
<th>Validation Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>OISTE Standard DV SSL Certificate</td>
<td>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.</td>
</tr>
<tr>
<td>OISTE Advanced OV SSL Certificate</td>
<td>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.</td>
</tr>
<tr>
<td>OISTE Advanced EV SSL Certificate</td>
<td>The Issuing CA must apply the requirements of section 11.8.3 of the EV Guidelines.</td>
</tr>
</tbody>
</table>

3.2.6 Criteria for interoperation

As stipulated in the CPS published by the Issuing CA.

3.3 Identification and Authentication for Re-key Requests

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

3.3.1 Identification and authentication for routine re-key

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

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

The 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).

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and Authentication for Revocation Requests

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

4.1 Certificate Application

As stipulated in the CPS published by the Issuing CA.

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 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.

4.2 Certificate Application Processing

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

4.2.1 Performing identification and authentication functions

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.

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 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.

4.2.3 Time to process certificate applications

There is no time limit stipulated to complete the processing of an application.
4.3 Certificate Issuance
An approved certificate request will be processed by the authorized responsible.

4.3.1 CA actions during certificate issuance
As stipulated in the CPS published by the Issuing CA.

4.3.2 Notifications to subscriber by the CA of issuance of certificate
As stipulated in the CPS published by the Issuing CA.

4.4 Certificate Acceptance
As stipulated in the CPS published by the Issuing CA.

4.4.1 Conduct constituting certificate acceptance
As stipulated in the CPS published by the Issuing CA.

4.4.2 Publication of the certificate by the CA
The CAs operating under the OGTM publish all issued certificates as specified in section 2 of this document.

4.4.3 Notification of certificate issuance by the CA to other entities
As stipulated in the CPS published by the Issuing CA.

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

4.5.1 Subscriber private key and certificate usage
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.

4.5.2 Relying party public key and certificate usage
As stipulated in the CPS published by the Issuing CA.

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.
4.6.1 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.

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

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

4.6.4 Notification of new certificate issuance to subscriber
As stipulated in the CPS published by the Issuing CA.

4.6.5 Conduct constituting acceptance of a renewal certificate
As stipulated in the CPS published by the Issuing CA.

4.6.6 Publication of the renewal certificate by the CA
The CAs operating under the OGTM publish all issued certificates as specified in section 2 of this document.

4.6.7 Notification of certificate issuance by the CA to other entities
As stipulated in the CPS published by the Issuing CA.

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

4.7.1 Circumstance for certificate re-key
Any certificate that is not revoked can be re-keyed.

4.7.2 Who may request certification of a new public key
The certificate renewal can be requested by the same entities allowed to request the first issuance of the certificate.

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

4.7.4 Notification of new certificate issuance to subscriber
As stipulated in the CPS published by the Issuing CA.

4.7.5 Conduct constituting acceptance of a re-keyed certificate
As stipulated in the CPS published by the Issuing CA.
4.7.6 Publication of the re-keyed certificate by the CA

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

4.7.7 Notification of certificate issuance by the CA to other entities

As stipulated in the CPS published by the Issuing CA.

4.8 Certificate Modification

The OGT M 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

Does not apply.

4.8.2 Who may request certificate modification

Does not apply.

4.8.3 Processing certificate modification requests

Does not apply.

4.8.4 Notification of new certificate issuance to subscriber

Does not apply.

4.8.5 Conduct constituting acceptance of modified certificate

Does not apply.

4.8.6 Publication of the modified certificate by the CA

Does not apply.

4.8.7 Notification of certificate issuance by the CA to other entities

Does not apply.

4.9 Certificate Revocation and Suspension

All Certification Authorities operating under the OGT M 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.
4.9.1 Circumstances for revocation
As stipulated in the CPS published by the Issuing CA.

4.9.2 Who can request revocation
As stipulated in the CPS published by the Issuing CA.

4.9.3 Procedure for revocation request
As stipulated in the CPS published by the Issuing CA.

4.9.4 Revocation request grace period
As stipulated in the CPS published by the Issuing CA.

4.9.5 Time within which CA must process the revocation request
As stipulated in the CPS published by the Issuing CA.

4.9.6 Revocation checking requirement for relying parties
As stipulated in the CPS published by the Issuing CA.

4.9.7 CRL issuance frequency
As stipulated in the CPS published by the Issuing CA.

4.9.8 Maximum latency for CRLs
As stipulated in the CPS published by the Issuing CA.

4.9.9 On-line revocation/status checking availability
As stipulated in the CPS published by the Issuing CA.

4.9.10 On-line revocation checking requirements
As stipulated in the CPS published by the Issuing CA.

4.9.11 Other forms of revocation advertisements available
No stipulations.

4.9.12 Special requirements regarding key compromise
As stipulated in the CPS published by the Issuing CA.

4.9.13 Circumstances for suspension
Suspension is not permitted for SSL Certificates.

4.9.14 Who can request suspension
Does not apply.

4.9.15 Procedure for suspension request
Does not apply.
4.9.16 Limits on suspension period

*Does not apply.*

4.10 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.

4.10.1 Operational characteristics

*As stipulated in the CPS published by the Issuing CA.*

4.10.2 Service availability

*As stipulated in the CPS published by the Issuing CA.*

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

*As stipulated in the CPS published by the Issuing CA.*

4.12 Key Escrow and Recovery

Key escrow is not permitted for SSL Certificates.

4.12.1 Key escrow and recovery policy and practices

*Does not apply.*

4.12.2 Session key encapsulation and recovery policy and practices

*Does not apply.*
5 Management, Operational, and Physical Controls
As stipulated in the CPS published by the Issuing CA.

5.1 Physical Security Controls
As stipulated in the CPS published by the Issuing CA.

5.1.1 Site location and construction
As stipulated in the CPS published by the Issuing CA.

5.1.2 Physical access
As stipulated in the CPS published by the Issuing CA.

5.1.3 Power and air conditioning
As stipulated in the CPS published by the Issuing CA.

5.1.4 Water exposures
As stipulated in the CPS published by the Issuing CA.

5.1.5 Fire prevention and protection
As stipulated in the CPS published by the Issuing CA.

5.1.6 Media storage
As stipulated in the CPS published by the Issuing CA.

5.1.7 Waste disposal
As stipulated in the CPS published by the Issuing CA.

5.1.8 Backup
As stipulated in the CPS published by the Issuing CA.

5.2 Procedural Controls
As stipulated in the CPS published by the Issuing CA.

5.2.1 Trusted roles
As stipulated in the CPS published by the Issuing CA.

5.2.2 Number of persons required per task
As stipulated in the CPS published by the Issuing CA.

5.2.3 Identification and authentication for each role
As stipulated in the CPS published by the Issuing CA.
5.2.4 Roles requiring separation of duties
As stipulated in the CPS published by the Issuing CA.

5.3 Personnel Security Controls
As stipulated in the CPS published by the Issuing CA.

5.3.1 Qualifications, experience, and clearance requirements
As stipulated in the CPS published by the Issuing CA.

5.3.2 Background check procedures
As stipulated in the CPS published by the Issuing CA.

5.3.3 Training requirements
As stipulated in the CPS published by the Issuing CA.

5.3.4 Retraining frequency and requirements
As stipulated in the CPS published by the Issuing CA.

5.3.5 Job rotation frequency and sequence
As stipulated in the CPS published by the Issuing CA.

5.3.6 Sanctions for unauthorized actions
As stipulated in the CPS published by the Issuing CA.

5.3.7 Independent contractor requirements
As stipulated in the CPS published by the Issuing CA.

5.3.8 Documentation supplied to personnel
As stipulated in the CPS published by the Issuing CA.

5.3.9 Contract termination and assigned role change procedures
As stipulated in the CPS published by the Issuing CA.

5.4 Audit Logging Procedures
As stipulated in the CPS published by the Issuing CA.

5.4.1 Types of events recorded
As stipulated in the CPS published by the Issuing CA.

5.4.2 Frequency of processing log
As stipulated in the CPS published by the Issuing CA.
5.4.3 Retention period for audit log
As stipulated in the CPS published by the Issuing CA.

5.4.4 Protection of audit log
As stipulated in the CPS published by the Issuing CA.

5.4.5 Audit log backup procedures
As stipulated in the CPS published by the Issuing CA.

5.4.6 Audit collection system (internal vs. external)
As stipulated in the CPS published by the Issuing CA.

5.4.7 Notification to event-causing subject
As stipulated in the CPS published by the Issuing CA.

5.4.8 Vulnerability assessments
As stipulated in the CPS published by the Issuing CA.

5.5 Records Archival
As stipulated in the CPS published by the Issuing CA.

5.5.1 Types of records archived
As stipulated in the CPS published by the Issuing CA.

5.5.2 Retention period for archive
As stipulated in the CPS published by the Issuing CA.

5.5.3 Protection of archive
As stipulated in the CPS published by the Issuing CA.

5.5.4 Archive backup procedures
As stipulated in the CPS published by the Issuing CA.

5.5.5 Requirements for time-stamping of records
As stipulated in the CPS published by the Issuing CA.

5.5.6 Archive collection system (internal or external)
As stipulated in the CPS published by the Issuing CA.

5.5.7 Procedures to obtain and verify archive information
As stipulated in the CPS published by the Issuing CA.
5.6 Key Changeover
As stipulated in the CPS published by the Issuing CA.

5.7 Compromise and Disaster Recovery
As stipulated in the CPS published by the Issuing CA.

5.7.1 Incident and compromise handling procedures
As stipulated in the CPS published by the Issuing CA.

5.7.2 Computing resources, software, and/or data are corrupted
As stipulated in the CPS published by the Issuing CA.

5.7.3 Entity private key compromise procedures
As stipulated in the CPS published by the Issuing CA.

5.7.4 Business continuity capabilities after a disaster
As stipulated in the CPS published by the Issuing CA.

5.8 CA or RA Termination
As stipulated in the CPS published by the Issuing CA.
6 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.

6.1 Key Pair Generation and Installation

Under the OGMT, 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 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.

6.1.2 Private key delivery to subscriber

As stipulated in the CPS published by the Issuing CA.

6.1.3 Public key delivery to certificate issuer

As stipulated in the CPS published by the Issuing CA.

6.1.4 CA public key delivery to relying parties

As stipulated in the CPS published by the Issuing CA.

6.1.5 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.

6.1.6 Public key parameters generation and quality checking

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

6.1.7 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.

6.2 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.
6.2.1 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.

6.2.2 Private key (n out of m) multi-person control
As stipulated in the CPS published by the Issuing CA.

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

6.2.4 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.

6.2.5 Private key archival
The CA shall not provide key archival services.

6.2.6 Private key transfer into or from a cryptographic module
No stipulation

6.2.7 Private key storage on cryptographic module
No stipulation additional to the requirements expressed in section 6.1.

6.2.8 Method of activating private key
As stipulated in the CPS published by the Issuing CA.

6.2.9 Method of deactivating private key
As stipulated in the CPS published by the Issuing CA.

6.2.10 Method of destroying private key
As stipulated in the CPS published by the Issuing CA.

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
As stipulated in the CPS published by the Issuing CA.

6.3.2 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.
6.4 Activation Data
As stipulated in the CPS published by the Issuing CA.

6.4.1 Activation data generation and installation
As stipulated in the CPS published by the Issuing CA.

6.4.2 Activation data protection
As stipulated in the CPS published by the Issuing CA.

6.4.3 Other aspects of activation data
No stipulation.

6.5 Computer Security Controls
As stipulated in the CPS published by the Issuing CA.

6.5.1 Specific computer security technical requirements
As stipulated in the CPS published by the Issuing CA.

6.5.2 Computer security rating
As stipulated in the CPS published by the Issuing CA.

6.6 Life Cycle Security Controls
As stipulated in the CPS published by the Issuing CA.

6.6.1 System development controls
As stipulated in the CPS published by the Issuing CA.

6.6.2 Security management controls
As stipulated in the CPS published by the Issuing CA.

6.6.3 Life cycle security controls
As stipulated in the CPS published by the Issuing CA.

6.7 Network Security Controls
As stipulated in the CPS published by the Issuing CA.

6.8 Time-stamping
As stipulated in the CPS published by the Issuing CA.
7 Certificate and CRL Profiles

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

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 (“RFC 5280”).

7.1 Certificate Profile

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

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

The different extension profiles for SSL Certificates are listed below.

7.1.2.1 **OISTE Standard DV SSL Certificate**

<table>
<thead>
<tr>
<th>Extension Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority Key Identifier</td>
<td>Extension marked non-critical.</td>
</tr>
<tr>
<td>Key Identifier</td>
<td>&lt;KeyID&gt;</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>Extension marked non-critical</td>
</tr>
<tr>
<td>Key Identifier</td>
<td>The Subject Key Identifier of the Subject of this certificate.</td>
</tr>
<tr>
<td>CRL Distribution Point</td>
<td>Extension marked non-critical.</td>
</tr>
<tr>
<td>Full name</td>
<td>[1]CRL Distribution Point</td>
</tr>
<tr>
<td></td>
<td>Distribution Point Name:</td>
</tr>
<tr>
<td></td>
<td>Full Name:</td>
</tr>
<tr>
<td></td>
<td>URL=&lt;URL-TO-CRL&gt;</td>
</tr>
<tr>
<td>Policy Qualifier</td>
<td>See section Policy Qualifiers</td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>Extension marked non-critical.</td>
</tr>
<tr>
<td>Extensions</td>
<td>[1]Authority Info Access</td>
</tr>
<tr>
<td></td>
<td>Access Method=Certification Authority Issuer</td>
</tr>
<tr>
<td></td>
<td>(1.3.6.1.5.5.7.48.2)</td>
</tr>
<tr>
<td></td>
<td>Alternative Name:</td>
</tr>
<tr>
<td></td>
<td>URL=&lt;URL-TO-ISSUER-CERT&gt;</td>
</tr>
<tr>
<td>Key Usage</td>
<td>Extension marked critical.</td>
</tr>
<tr>
<td></td>
<td>Value: Digital Signature, Key Encipherment (a0)</td>
</tr>
<tr>
<td>Extended Key Usage</td>
<td>Client Authentication, Server Authentication</td>
</tr>
<tr>
<td>SubjectAltName</td>
<td>&lt;List of SAN&gt; (at least one)</td>
</tr>
</tbody>
</table>
### 7.1.2.2 OISTE Advanced OV SSL Certificate

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority Key Identifier</td>
<td>Extension marked non-critical.</td>
</tr>
<tr>
<td>Key Identifier</td>
<td>&lt;KeyID&gt;</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>Extension marked non-critical</td>
</tr>
<tr>
<td>Key Identifier</td>
<td>The Subject Key Identifier of the Subject of this certificate.</td>
</tr>
<tr>
<td>CRL Distribution Point</td>
<td>Extension marked non-critical.</td>
</tr>
<tr>
<td><strong>Full name</strong></td>
<td>[1]CRL Distribution Point</td>
</tr>
<tr>
<td></td>
<td>Distribution Point Name:</td>
</tr>
<tr>
<td></td>
<td>Full Name:</td>
</tr>
<tr>
<td></td>
<td>URL=&lt;URL-TO-CRL&gt;</td>
</tr>
<tr>
<td>Policy Qualifier</td>
<td>See Section Policy Qualifiers</td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>Extension marked non-critical.</td>
</tr>
<tr>
<td><strong>Extensions</strong></td>
<td>[1]Authority Info Access</td>
</tr>
<tr>
<td></td>
<td>Access Method=Certification Authority Issuer</td>
</tr>
<tr>
<td></td>
<td>(1.3.6.1.5.5.7.48.2)</td>
</tr>
<tr>
<td></td>
<td>Alternative Name:</td>
</tr>
<tr>
<td></td>
<td>URL=&lt;URL-TO-ISSUER-CERT&gt;</td>
</tr>
<tr>
<td>Key Usages</td>
<td>Extension marked critical.</td>
</tr>
<tr>
<td></td>
<td>Value: Data Encipherment, Digital Signature, Key Encipherment</td>
</tr>
<tr>
<td>Extended Key Usage</td>
<td>Client Authentication, Server Authentication</td>
</tr>
<tr>
<td>SubjectAltName</td>
<td>&lt;List of SAN&gt; (at least one)</td>
</tr>
</tbody>
</table>

### 7.1.2.3 OISTE Advanced EV SSL Certificate

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority Key Identifier</td>
<td>Extension marked non-critical.</td>
</tr>
<tr>
<td>Key Identifier</td>
<td>&lt;KeyID&gt;</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>Extension marked non-critical</td>
</tr>
<tr>
<td>Key Identifier</td>
<td>The Subject Key Identifier of the Subject of this certificate.</td>
</tr>
<tr>
<td>CRL Distribution Point</td>
<td>Extension marked non-critical.</td>
</tr>
<tr>
<td><strong>Full name</strong></td>
<td>[1]CRL Distribution Point</td>
</tr>
<tr>
<td></td>
<td>Distribution Point Name:</td>
</tr>
<tr>
<td></td>
<td>Full Name:</td>
</tr>
<tr>
<td></td>
<td>URL=&lt;URL-TO-CRL&gt;</td>
</tr>
<tr>
<td>Policy Qualifier</td>
<td>See Section Policy Qualifiers</td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>Extension marked non-critical.</td>
</tr>
<tr>
<td><strong>Extensions</strong></td>
<td>[1]Authority Info Access</td>
</tr>
<tr>
<td></td>
<td>Access Method=Certification Authority Issuer</td>
</tr>
<tr>
<td></td>
<td>(1.3.6.1.5.5.7.48.2)</td>
</tr>
<tr>
<td></td>
<td>Alternative Name:</td>
</tr>
<tr>
<td></td>
<td>URL=&lt;URL-TO-ISSUER-CERT&gt;</td>
</tr>
<tr>
<td>Key Usages</td>
<td>Extension marked critical.</td>
</tr>
<tr>
<td></td>
<td>Value: Data Encipherment, Digital Signature, Key Encipherment</td>
</tr>
<tr>
<td>Extended Key Usage</td>
<td>Client Authentication, Server Authentication</td>
</tr>
<tr>
<td>SubjectAltName</td>
<td>&lt;List of SAN&gt; (at least one)</td>
</tr>
</tbody>
</table>
7.1.3 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}
  ```

7.1.4 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.

7.1.5 Name constraints

No stipulation for subscriber certificates.

7.1.6 Certificate policy object identifier

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

7.1.7 Usage of Policy Constraints extension

No stipulation for subscriber certificates. The CA can disclose additional stipulations in its CPS for CA certificates.
7.1.8 Policy qualifiers syntax and semantics
No stipulation for subscriber certificates. The CA can disclose additional stipulations in its CPS for CA certificates.

7.1.9 Processing semantics for the critical Certificate Policies extension
The “Certificate Policy” extension identifies the Policy that the OGTM assigned explicitly to a certificate profile. Software Applications requiring a specific certificate profile to process a digital signature must check this extension in order to verify the suitability of the certificate for the intended purpose.

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

7.2.1 Version number(s)
CRLs conforming to X.509 Version 2 are supported in the OGTM.

7.2.2 CRL Profile and CRL entry extensions
CRL must include the following minimum extensions, as defined by the above standard:

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

7.3 OCSP Profile
Issuing CAs are mandated to provide OCSP service at all types of SSL Certificates.

7.3.1 Version number(s)
OGTM provides support for Version 1 of RFC6960.

7.3.2 OCSP extensions
No stipulation.
8 Compliance Audit and Other Assessment

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.

8.1 Frequency or circumstances of assessment
As stipulated in the CPS published by the Issuing CA.

8.2 Identity/qualifications of assessor
As stipulated in the CPS published by the Issuing CA.

8.3 Assessor's relationship to assessed entity
As stipulated in the CPS published by the Issuing CA.

8.4 Topics covered by assessment
As stipulated in the CPS published by the Issuing CA.

8.5 Actions taken as a result of deficiency
As stipulated in the CPS published by the Issuing CA.

8.6 Communication of results
As stipulated in the CPS published by the Issuing CA.
9 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.

9.1 Fees

As stipulated in the CPS published by the Issuing CA.

9.1.1 Certificate issuance or renewal fees

As stipulated in the CPS published by the Issuing CA.

9.1.2 Certificate access fees

As stipulated in the CPS published by the Issuing CA.

9.1.3 Revocation or status information access fees

As stipulated in the CPS published by the Issuing CA.

9.1.4 Fees for other services

As stipulated in the CPS published by the Issuing CA.

9.1.5 Refund policy

As stipulated in the CPS published by the Issuing CA.

9.2 Financial Responsibility

As stipulated in the CPS published by the Issuing CA.

9.2.1 Insurance coverage

As stipulated in the CPS published by the Issuing CA.

9.2.2 Other assets

As stipulated in the CPS published by the Issuing CA.

9.2.3 Insurance or warranty coverage for end-entities

As stipulated in the CPS published by the Issuing CA.

9.3 Confidentiality of Business Information

As stipulated in the CPS published by the Issuing CA.

9.3.1 Scope of confidential information

As stipulated in the CPS published by the Issuing CA.

9.3.2 Information not within the scope of confidential information

As stipulated in the CPS published by the Issuing CA.
9.3.3 Responsibility to protect confidential information
As stipulated in the CPS published by the Issuing CA.

9.4 Privacy of Personal Information
As stipulated in the CPS published by the Issuing CA.

9.4.1 Privacy plan
As stipulated in the CPS published by the subordinate CA.

9.4.2 Information treated as private
As stipulated in the CPS published by the Issuing CA.

9.4.3 Information not deemed private
As stipulated in the CPS published by the Issuing CA.

9.4.4 Responsibility to protect private information
As stipulated in the CPS published by the Issuing CA.

9.4.5 Notice and consent to use private information
As stipulated in the CPS published by the Issuing CA.

9.4.6 Disclosure pursuant to judicial or administrative process
As stipulated in the CPS published by the Issuing CA.

9.4.7 Other information disclosure circumstances
As stipulated in the CPS published by the Issuing CA.

9.5 Intellectual Property Rights
As stipulated in the CPS published by the Issuing CA.

9.6 Representations and Warranties
As stipulated in the CPS published by the Issuing CA.

9.6.1 CA representations and warranties
As stipulated in the CPS published by the Issuing CA.

9.6.2 RA representations and warranties
As stipulated in the CPS published by the Issuing CA.

9.6.3 Subscriber representations and warranties
As stipulated in the CPS published by the Issuing CA.
9.6.4 Relying party representations and warranties
As stipulated in the CPS published by the Issuing CA.

9.6.5 Representations and warranties of other participants
As stipulated in the CPS published by the Issuing CA.

9.7 Disclaimers of Warranties
As stipulated in the CPS published by the Issuing CA.

9.8 Limitations of Liability
As stipulated in the CPS published by the Issuing CA.

9.9 Indemnities
As stipulated in the CPS published by the Issuing CA.

9.10 Term and Termination
As stipulated in the CPS published by the Issuing CA.

9.10.1 Term
As stipulated in the CPS published by the Issuing CA.

9.10.2 Termination
As stipulated in the CPS published by the Issuing CA.

9.10.3 Effect of termination and survival
As stipulated in the CPS published by the Issuing CA.

9.11 Individual notices and communications with participants
As stipulated in the CPS published by the Issuing CA.

9.12 Amendments
As stipulated in the CPS published by the Issuing CA.

9.12.1 Procedure for amendment
As stipulated in the CPS published by the Issuing CA.

9.12.2 Notification mechanism and period
As stipulated in the CPS published by the Issuing CA.

9.12.3 Circumstances under which OID must be changed
As stipulated in the CPS published by the Issuing CA.
9.13 Dispute Resolution Procedures
As stipulated in the CPS published by the Issuing CA.

9.14 Governing Law
As stipulated in the CPS published by the Issuing CA.

9.15 Compliance with Applicable Law
As stipulated in the CPS published by the Issuing CA.

9.16 Miscellaneous Provisions
As stipulated in the CPS published by the Issuing CA.

9.16.1 Entire agreement
As stipulated in the CPS published by the Issuing CA.

9.16.2 Assignment
As stipulated in the CPS published by the Issuing CA.

9.16.3 Severability
As stipulated in the CPS published by the Issuing CA.

9.16.4 Enforcement (attorneys’ fees and waiver of rights)
As stipulated in the CPS published by the Issuing CA.

9.16.5 Force Majeure
As stipulated in the CPS published by the Issuing CA.

9.17 Other Provisions
As stipulated in the CPS published by the Issuing CA.
### 10 Annex A: Glossary

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