Consorci
Administració Oberta
de Catalunya

Certification Practices Statement
Public Sector Certification Entity
(EC-SECTORPUBLIC)

Reference:: D1111_E0650_N-DPC EC-SECTORPUBLIC

Version: 2.0

Date: 09/05/2018

Index

1. Introduction

1.1. Presentation

1.1.1. Certification types and classes

The Consorci AOC has defined a certification services typology that allows the EC-SECTORPUBLIC to issue digital certificates for diverse uses towards various types of end user.

The profiles contained in this document have been created in order to comply with the requirements stipulated in applicable law, which is described in section 9.15 Conformity with applicable law.

End-User certificates are divided into:

- Infrastructure certificates, defined by the fact that the private key owner is an infrastructure operator, and that the associated certificate is used to authorise operations related to certification services such as the approval of certification requests.
- Personal certificates, defined by the fact that the private key owner is a physical person, who acts on behalf of the subscriber or holder of the certificate (who could be the same, or a legal person to which the certificate is linked).
- Device certificates, defined by the fact that the private key owner is an IT device which automatically executes signature and decode operations, under the responsibility of a physical or legal person (the named subscriber or holder of the certificate).

When the certificates are issued in THE INSTITUTIONS it is required to follow the authentication procedures of the certificate organization holder, since related to corporate certificates, in which the certificate subscriber organization and the Entity coincide.

In exceptional circumstances, motivated by the need to guarantee the security of the person who is identifying or signing, it is possible to utilise an pseudonym in special cases (such as certificates for security bodies or justice administration affiliated personnel) in accordance with the provisions of the Regulation (EU) Nº 910/2014 of the European Parliament and the Council of Europe, 23th of July 2014, related to electronic identification and trusted services for the electronic transactions within the internal market and repealing the Directive 1999/93/CE to applicable law (described in section 9.15 Conformity with applicable law).

In these cases, the key owner will be identified directly by using an identifier that validates the identification of the acting person, under specific requirement of the competent authority for this purpose.

For all other cases, the Certification Entity needs to validate, prior to issue and delivery of a certificate, the identity of the subscriber and the private key owner, and other required data corresponding to corporate certificates. Subscribers can be individuals (when they are issued to a physical person in their own name - for example to citizens in order to relate by electronic media towards the entities of the public sector of Catalonia) or corporate (relating

to organizations from either the private or public sector outside Catalonia - when they are issued to an organization that acts by means of a physical person, this is identified in the certificate even if an pseudonym is used).

1.1.1.1. Infrastructure certificates

The EC-SECTORPUBLIC issues the following types of infrastructure certificates:

- Personal infrastructure certificates for operator identification and qualified electronic signature (CIPISQ), used for authorising operations related to certification services such as certification request approval.
- Infrastructure certificate for servers used for online certificates status (CIO), used by a server OCSP Responder to sign responses regarding certificate validity status.

1.1.1.2. Personal certificates

The EC-SECTORPUBLIC issues the following types of personal certificates:

- High-level authentication electronic certificate for public servant: this is a qualified certificate that works with qualified electronic signature creation devices. The certificate guarantees the identity of the subscriber and the owner of the private key of identification and signature, and can be used with applications that do not require the electronic signature equivalent of a handwritten signature, but instead just require the key owner identification on behalf of the subscribers.
- High-level qualified certificate of signature for public servant: a qualified certificate that. works with qualified electronic signature creation devices. The certificate guarantees the identity of the subscriber and the owner of the private key of signature, and allows the generation of a “qualified electronic signature” written for legal effect without the need of be compliant with any additional requirement.
- High-level electronic certificate for affiliated person: a qualified certificate that works with qualified electronic signature creation device. The certificate guarantees the identity of the subscriber and the owner of the private key of signature and identity, and allows the authentication and the generation of the “qualified electronic signature”.
- High-level authentication electronic certificate for public servant with pseudonym: this is a qualified certificate issued in accordance with the provisions of applicable law, (as described in section 9.15 Conformity with applicable law) to be used with qualified electronic signature creation devices. The certificate guarantees, in an indirect form, the identity of the subscriber and the owner of the private key of identification. These certificates can be used within applications that do not require the electronic signature equivalent of a handwritten signature, but instead just require key owner identification on behalf of the subscribers.
- High-level authentication qualified certificate of signature for public servant with pseudonym: this is a qualified certificate issued in accordance with the provisions of applicable law (as described in section 9.15 Conformity with the applicable law) which works with qualified electronic signature creation devices. The certificate guarantees, in an indirect form, the identity of the subscriber and owner of the

private key of signature, and allows the generation of a “qualified electronic signature”.

- High-level electronic certificate for representatives towards Public Administrations: this is a qualified certificate issued in accordance with the provisions of applicable law (as described in section 9.15 Conformity with applicable law) which works with qualified electronic signature creation devices. The certificate guarantees the identity of the subscriber and the owner of the private key of signature and identification, and allows the generation of a “qualified electronic signature”. The certificate can also be used in applications that do not require the electronic signature equivalent of a handwritten signature, but only require key owner identification on behalf of the subscribers.
- Mid-level electronic certificate for public servant and for affiliated person: this is a qualified certificate issued in accordance with the provisions of applicable legislation, (as described in section 9.15 Conformity with the applicable law) that guarantees the identity of the subscriber, owner of the private key of signature and identification, and allows the generation of an “advanced electronic signature”.

1.1.1.3. Device certificates

The EC-SECTORPUBLIC issues the following types of device certificates:

- Secure sockets device certificate (CDS-1), used for IT applications that utilise SSL or TLS server for identification of connecting client applications and for securing the communications between client and server.
- Secure sockets of Extended Validation device certificate (CDS-1 EV), used for an IT applications that utilise, SSL or TLS server for identification towards connecting client applications and for securing the communications between client and server, offering the automatic validation in the browser.
- Mid-level electronic office device certificate (CDS-1 SENM), used for identifying and guaranteeing a secure communication with an entity electronic office.

  This certificate can be used in various ways such as for citizens secure connection with official websites, website authentication, electronic register hosting, representation registers enquiry and authorisation.

  Mid-level certificate is recommended by the majority of public administrations while accepting the following risks: security violation (for example identity theft), moderate economic losses, loss of sensitive or critical information, refutation of a transaction with significant economic impact.
- Application device certificate (CDA-1), stored on a server and required by an application, it signs documents or messages.
- Mid-level device certificate of public right Administration, Authority or Entity electronic seal, used for identification and authentication of the competency exercise in automated administration.

  Examples of usage for this certificate include for data exchange between administrations, for the identification and authentication of a system, web service or application, for automated electronic archive or electronic certified copy

Mid-level certificate is recommended by the majority of public administrations while accepting the following risks: security violation (for example identity theft), moderate economic losses, loss of sensitive or critical information, refutation of a transaction with significant economic impact.

1.1.1.4. Test certificates

It is possible to issue test certificates for all types of certificates defined within this policy.

1.1.2. Relation between the Certification Practice Statement (CPS) and other documents

This document contains the certification practice statement of the EC-SECTOR PUBLIC.

The EC-SECTORPUBLIC issues certificates within the operated certification hierarchy of the Consorci AOC, which prescribes the need to have a declaration of certification practices according to the certification general policy of the Consorci AOC. .

This Certification Practice Statement (CPS) includes procedures that the EC-SECTORPUBLIC applies in the provision of its services, in accordance with the established requirements of the managed policies and the applicable law.

This CPS is compliant with Certification General Policy, and includes multiple references to this policy in order to avoid duplications where the CPS does not introduce additional information.

1.2. Document name and identification

1.2.1. Identification of this document

This document is named “Certification Practice Statement (CPS) of l’EC-SECTORPUBLIC”.

This Certification Practice Statement is identified by the following OID:

```
1.3.6.1.4.1.15096.1.2.10
```

1.2.2. Identification of certification policies covered by this CPS

L’EC-SECTORPUBLIC issues and manages certificates in accordance with the following policies:

Personal certificates:

- **CPI-1** – High-level authentication electronic certificate for public servant, issued by the EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.7.1.2

- **CPSQ-1** – High-level signature qualified certificate for public servant

  OID: 1.3.6.1.4.1.15096.1.3.2.7.1.1

- **CPISQ-2** – High-level electronic certificate for affiliated person

  OID: 1.3.6.1.4.1.15096.1.3.2.82.1

- **CPISA** – Mid-level electronic certificate, issued by the EC-SECTORPUBLIC

  Public servant – CPISA-1 - OID: 1.3.6.1.4.1.15096.1.3.2.7.3.1

  Affiliated person – CPISA-2 - OID: 1.3.6.1.4.1.15096.1.3.2.86.1

- **CPPI-1** – High-level authentication electronic certificate for public servant with pseudonym, issued by the EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.4.1.2

- **CPPSQ-1** – High-level signature qualified certificate for public servant with pseudonym, issued by the EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.4.1.1

- **CPRISQ-1** – High-level electronic certificate for representative towards public administration, issued by the EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.8.1.1

Device certificates:

- **CDS-1** – Device certificate SSL, issued by the EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.51.1

- **CDSQ-1** - Device certificate SSL EV, issued by the EC-SECTORPUBLIC. These certificates can not be issued after the entry into force of version 2.0 of this document.

  OID: 1.3.6.1.4.1.15096.1.3.1.51.2

- **CDSQ-1** - Device certificate SSL EV, issued by the EC-SECTORPUBLIC and adapted to eIDAS

  OID: 1.3.6.1.4.1.15096.1.3.2.51.2

- **CDS-1 SENM -** Mid-level electronic office certificate, issued by the EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.5.2

- **CDA-1** – Application certificate, issued by the EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.91.1

- **CDA-1 SGNM -** Mid-level electronic seal certificate, issued by the EC-SECTORPUBLIC

  OID: 1.3.6.1.4.1.15096.1.3.2.6.2

The documents describing these certificate profiles are published in the Consorci AOC website.

1.3. Certificate users community

This Certification Practice Statement regulates user community members who obtain certificates in order to perform administrative relations by electronic media, in accordance with applicable law and the corresponding administrative normative (as are described in section 9.15 Conformity with applicable law).

EC-SECTORPUBLIC certificates are not issued to individuals, but for entities, personnel and the entity devices involved the Public Sector of Catalonia.

1.3.1. Certification services providers

A certification service provider is a physical or legal person who issues certificates and provides other services related to electronic signature, in accordance with applicable law (as, described in section 9.15 Conformity with the applicable law).

Consorci AOC will be the certification services provider of the EC-SECTORPUBLIC.

According to this role, the Consorci AOC is responsible for the activity of the CEC-SECTORPUBLIC towards end users and third party certificates and electronic signatures verifiers.

1.3.2. Certification Root Entity

Consorci AOC has the main certification authority, which is the root of the certification public hierarchy of Catalonia: the EC-ACC, the purpose of which is to integrate other certification entities in the Catalan public system of certification via technical connection of the corresponding certification authorities.

1.3.3. EC-SECTORPUBLIC

EC-SECTORPUBLIC is the Certification Entity which provides digital certificates to entities, the personnel of those entities and units of the Organizations, Departments and Public Companies that integrate the Public Sector of Catalonia.

EC-SECTORPUBLIC is connected to the certification entities hierarchy of Catalonia public entities and issues the certificates indicated in section 1.1.1.

1.3.4. Register Entities

In accordance with the provisions of the Certification General Policy, the Register Entities support the Affiliate Certification Entities with specific procedures and relations with the certificate applicants and subscribers (especially in relation to identification processes, register and authentication of the certificate subscribers and key owners).

The Consorci AOC is responsible for the Register Entities creation process of the EC-SECTORPUBLIC: it verifies that the Register Entity has the required human and material resources, and has ensured the knowledge of personnel who will be responsible for the issuing of certificates (known as register entity operators). It is also responsible for the issuing of operator certificates (typically they will be CIPISQ); the Consorci AOC will validate requests for operator certificates of the Register Entities through analysis of content and proceeding with the necessary compliancy confirmations in accordance with the Certification General Policy and this Certificate Practice Statement.

The following Register Entities of the EC-SECTORPUBLIC exist:

1) The subscriber body, operated by a certificate subscriber entity.
2) The Register Entities, who shall cooperate with the EC-SECTORPUBLIC during the certificates issue process.

In order to become Register Entities, they are required to design and set the components and technical procedures, either legal or security, regarding the life cycle of signature secure devices, or to the life cycle of software support keys and certificates it issues for cases of encrypted secure devices. These components and procedures will be previously approved by the Consorci AOC.

1.3.5. End users

An End user is a physical or legal person who obtains and uses personal, entity and device certificates issued by the EC-SECTORPUBLIC; in particular the following end users can be differentiated:

- Certificate applicants
- Certificate subscribers or certificate holders
- Key owners
- Signature and certificate verifiers

1.3.5.1. Certificate applicants

In accordance with the provisions of the Certification General Policy. In particular, the types of certificate applicants of the ES-SECTORPUBLIC are:

a) A person authorised by the future subscriber entity: corporate certificates

b) A person authorised by the Certification Entity - typically this would be the Consorci AOC acting of its own accord.

The authorisation must be formalised throughout the document.

1.3.5.2. Certificate subscribers

In accordance with the provisions of the Certification General Policy.

1.3.5.3. Key owners

In accordance with the provisions of the Certification General Policy.

1.3.5.4. Certificate users

In accordance with the provisions of the Certification General Policy.

1.3.5.5. Certificate verifiers

In accordance with the provisions of the Certification General Policy.

1.4. Use of the certificates

This sections lists the typical applied uses of each type of certificate, while settings limits and prohibiting certain certificate applications.

1.4.1. Typical use of the certificates

1.4.1.1. Infrastructure Certificates

1.4.1.1.1. Infrastructure personal Certificate of identification and qualified signature (CIPISQ)

In accordance with the provisions of the Certification General Policy.

1.4.1.1.2. Specific requirements for the CIC

In accordance with the provisions of the Certification General Policy.

1.4.1.1.3. Specific requirements for the CIO

In accordance with the provisions of the Certification General Policy.

1.4.1.2. Specific requirements for personal Certificates

1.4.1.2.1. High-level authentication electronic certificate for public servant

To allow user authentication.

1.4.1.2.2. High-level qualified certificate of signature for public servant

To allow a public servant to create a qualified electronic signature.

1.4.1.2.3. High-level electronic certificate for affiliate person

To allow an affiliated person to authenticate and initiate the creation of a qualified electronic signature.

1.4.1.2.4. Mid-level electronic certificate for public servant

These allow a public servant to authenticate and initiate the creation of a qualified electronic signature.

1.4.1.2.5. Mid-level electronic certificate for affiliate person

These allow the affiliated person to authenticate and initiate the creation of a qualified electronic signature.

1.4.1.2.6. High-level authentication electronic certificate fo public servant with pseudonym

These allow the authentication of public servants identified with pseudonym.

1.4.1.2.7. High-level qualified certificate of signature for public servant with pseudonym

These allow public servants identified with pseudonym, to generate qualified signatures.

1.4.1.2.8. High-level electronic certificate for representative towards the public administration

These allow public servers to authenticate with entitlement of public entity representatives, and also the generation of qualified electronic signature.

1.4.1.3. Device certificates

1.4.1.3.1. Device Certificates SSL (CDS-1)

The EC-SECTORPUBLIC will be able to issue certificates to public sector entities of Catalonia that are responsible for operation with secure sockets SSL or TLS, for the following uses:

- Server authentication
- Encryption of communications between client and server

These are ordinary certificates used to guarantee the origin of the communication (the identity of the specific server where they are installed), as well as the identity of the certificate responsible entity.

1.4.1.3.2. Device Certificates SSL EV (CDS-1 EV)

EC-SECTORPUBLIC issues certificates to public sector entities of Catalonia that are responsible for the operation with secure sockets SSL or TLS, with the following uses:

- Server authentication
- Encryption of communications between client and server
- Automatic validation of certification by means of web browsers attached to the CAB Forum.

These are ordinary certificates used to guarantee the origin of the communication (the identity of the specific server where they are installed), as well as the identity of the certificate responsible entity.

1.4.1.3.3. Mid-level electronic office certificate (CDS-1 SENM)

EC-SECTORPUBLIC issues certificates to public sector entities of Catalonia that are responsible for operations where secure sockets SSL or TLS is used for identifying and guaranteeing secure communication with their entity electronic offices. These are qualified certificates for validating official website authentication (the origin of the web connections between a citizen and an electronic office) and secure connection to this website, the hosting of in/out electronic registers, enquiry and authorisation of representation registers etc.

1.4.1.3.4. Application certificate (CDA-1)

EC-SECTORPUBLIC issues application certificates to public sector entities of Catalonia that are responsible for the operation of IT applications that identify digitally, signing of web services or other protocols electronically, and receive encrypted documents and messages.

These are ordinary certificates that guarantee the integrity and authenticity of the signed data. They also guarantee the identity of the responsible entity.

1.4.1.3.5. Mid-level electronic seal certificate (CDA-1 SGNM)

EC-SECTORPUBLIC shall issue them to Public Sector of Catalonia member entities, for identification and authentication of the competency exercise in automated administration.

This certificate can be used, for example, for data exchange between administrations, identification and authentication of a system, web service or application, for implementing automatic electronic archive systems supporting enquiries for electronic copies.

1.4.2. Prohibited applications

1.4.2.1. Information for all certificate types

The certificates have not been designed for, and should not allocated or authorised for, use or resell for dangerous control equipments or for uses that require error tests, like the functional control of nuclear installations, aerial communication or navigation systems, or arms control systems where a single mistake could result in death, personal injuries or severe environmental damage.

1.4.2.2. Infrastructure certificates

The use of the infrastructure certificates issued by the EC-SECTORPUBLIC - profiles of which are listed in section *1.2.2 Identification of certification policies covered by this CPS* - will not allowed for the purposes described in the Certification General Policy, section *Prohibited applications*.

1.4.2.3. Personal certificates

The use of the personal certificates issued by the EC-SECTORPUBLIC - which profiles are listed in section *1.2.2 Identification of certification policies covered by this CPS* - will not be allowed for the purposes described in the Certification General Policy, section *Prohibited applications*.

1.4.2.4. Device certificates

The use of the device certificates issued by the EC-SECTORPUBLIC - which profiles are listed in section *1.2.2 Identification of certification policies covered by this CPS* - will not be allowed for the purposes described in the Certification General Policy, section *Prohibited applications*.

1.5. Administration of the Practice Statement

1.5.1. Responsible organization for managing the specification

Consorci Administració Oberta de Catalunya – Consorci AOC

1.5.2. Contact details of the organization

Consorci Administració Oberta de Catalunya – Consorci AOC

Registered office: Via Laietana, 26 – 08003 Barcelona

Commercial postal address:: Tànger, 98, planta baixa (22@ Edifici Interface) - 08018 Barcelona

Website of the Consorci AOC: www.aoc.cat

User service contact: 902 901 080 (24x7 for certificate suspension management)

1.5.3. Responsible person deciding conformity of a Certification Practice Statement (CPS) with the policy

The person in charge of the SCD Service in the Consorci AOC decides on the conformity of a CPS with the Certification General Policy, based on the results of a third party audit twice yearly.

1.5.4. Approval procedure

The documentary and organization system of the EC-SECTORPUBLIC guarantees, by means of the existence and application of its corresponding procedures, the correct maintenance of the Certification Practice Statement and of the service specifications related with that CPS. This includes service specification modification and publication procedures.

The initial version of this Practice Statement is approved by the Executive Board of the Consorci AOC, which is the collegiate body of the Consorci Executive Management.
The Managing Director of the Consorci AOC shall have the competence to approve successive modifications of this Practice Statement.

2. Publication of information and certificates directory

2.1. Certificates Directory

In accordance with the provisions of the Certification General Policy.

2.2. Publication of the EC-SECTORPUBLIC information

In accordance with provisions of the Certification General Policy..

2.3. Publication frequency

EC-SECTORPUBLIC information is published as it becomes available, and immediately when references related to certifcate validity are issued

Changes to the document are governed in accordance with the provisions of section *9.12.1 Modifications procedure*.

Within 15 days of publication, the change reference is removed from the main website and inserted into the directory.

Archive versions of the documentation are preserved by EC-SECTORPUBLIC during a 15 year retention period, and are available for any applicant enquiry during that period.

Information about certificate revocation status is published in accordance with the provisions of section 4.10.7 Issue frequency of certificate revocation lists *(CRL's).*

2.4. Access control

In accordance with the provisions of the Certification General Policy..

3. Identification and authentication

3.1. Name management

This section outlines requirements related to identification and authentication procedures used during registration operations that the Register Entities execute before issuing and delivering the certificates.

3.1.1. Types of names

In accordance with the provisions of the Certification General Policy.

3.1.2. Meaning of the names

In accordance with the provisions of the Certification General Policy. .

3.1.3. Use of anonymous and pseudonym

The use of pseudonyms in order to identify an organization is not allowed. .

Personal certificates, either individual or corporate, may indicate pseudonym instead of the true name of the certificate key owner.

The pseudonym shall be stated unequivocally and its nature will be indicated in the description of the certificate.[1]

The pseudonym shall be stated through a field *Pseudonym* in the certificate, and will be linked to an email address using a mandatory field.

[1] Article 32 Regulations (EU) Nº 910/2014 of European Parliament of the Council, 23rd July 2014, regarding electronic identification and trusted services for electronic transactions in the domestic market, and repealing Directive 1999/93/CE.

However, the issue of certificates with pseudonym will guarantee, during the registration phase, the availability of the key owner real identification, which shall only be revealed once a previous competent authority request has been completed.

3.1.4. Interpretation of name formats

No additional stipulation required.

3.1.5. Uniqueness of names

In accordance with the provisions of the Certification General Policy. .

3.1.6. Resolution of conflicts related to names

In accordance with provisions within the Certification General Policy. .

Regarding the treatment of registered trademark, please refer to section 9.5.3.

3.2. Initial identity validation

3.2.1. Private key possession test

In accordance with the provisions of the Certification General Policy.

3.2.2. Authentication of organization identity

This section contains the requirements for checking the identity of an organization identified in the certificate.

Generally, the EC-SECTORPUBLIC does not need to decide if a certificate applicant has any rights regarding the name used in a certificate request. It will not act as an arbitrator or mediator, and it does not need to solve any conflict regarding person or organization names property, domain names, commercial brand or names (for example those related to email addresses).

3.2.2.1. Register entities

In accordance with the provisions of the Certification General Policy.

3.2.2.2. Subscriber entities of corporate certificates

Applying authentication procedures on the subscriber entities (certificate holder) in certificates issued to THE INSTITUTIONS is not required, due to that they are corporate certificates in where the certificate subscriber organization and the Register Entity coincide.

3.2.2.3. Other subscriber entities

3.2.2.3.1. Requirements for affiliate person certificates

In accordance with the provisions of the Certification General Policy..

3.2.2.3.2. Specific requirements for device certificates

In accordance with the provisions of the Certification General Policy.

3.2.3. Authentication of a physical person identity

This section contains information controlling the identification validation of a person identified in a certificate.

3.2.3.1. Identification elements

Each subscriber organization decides on the necessary documentation required for proving the key owner identity, and this is described in its governing regulations.

In each case, these identifying documents will contain at least:

- Name and surnames of the person
- Legally acknowledged identity number (National Id Document, VAT number or National Id for Foreigners of the Schengen Agreement countries; passport for cases of foreigner certificates).
- Any other information that could be used for differentiate one person from another, within the institution scope (for example: photography, email, category, position etc.).

3.2.3.2. Validation of the identification elements

In accordance with provisions of the Certification General Policy.

3.2.3.3. Necessity of personal presence

In accordance with provisions of the Certification General Policy.

3.2.3.4. Connection between physical person and organization

Certificates for public servant: these are corporate certificates where the Register Entity and the subscriber coincide, therefore it is not necessary to obtain specific documentary proof about the connection between the key owner and the Register Entity, since the entity inner registers shall be used.

Certificates for affiliate person: the EC-SECTORPUBLIC - by means of the intervention of a Register Entity - must obtain a documentary proof about the connection between the

organization and the physical person who will become the private key owner, through any media accepted within the law.

3.2.4. Information not verified

The certificate subscriber entity is responsible for all the information included in the certificate request being exact and correct for the certificate purpose, and that it has right for its use (for example, the right to use one name in the email address or the legitimacy in the use of a web server).

3.3. Identification and authentication of the renewal requests

3.3.1. Validation for certificates renewal

Regardless of whether an ordinary renewal or renewal after the revocation of a certificate is being made, the process for will be the same as for new certificates issue: the EC-SECTORPUBLIC will need to check - by means of a Register Entity intervention - that the information used to verify identity, plus the rest of the subscriber data and the key owner information remains valid.

If any information about the subscriber or the key owner has changed, it shall be registered, in accordance with the provisions in section *3.2 Initial identity validation*.

4. Operation features of the certificates life cycle

Note: the word "*notification*" is used as an equivalent of "*communication*" in this document, except for when used to reference documentary processes with other public organizations required by applicable law.

4.1. Request for certificate issue

Submission of request is the first step a potential subscriber takes towards obtaining certificates for its personnel.

For Public Administrations, the request shall be sent:

- through T-CAT Register Entities
- directly to the Consorci AOC (in cases where the requester does not have any allocated register entity, Consorci AOC will act as a T-CAT Register Entity).

The request application requires the submission of documentation containing exact and proven (certified) information regarding persons, entities or devices for which the certificate is to be used. The application needs to be signed by the subscriber entity authorised person to that purpose, and certification of the information needs to be attached.

It may also be necessary to confirm a physical address, or provide other additional data in order to establish the means for direct contact with the future key owner.

All documentation should be delivered to the Register Entity through electronic media, although it can be sent in paper format or via email in exceptional cases such us the following:

- the subscriber entity, due to its legal nature, is not able to utilise the IT application used for sending the requests (currently, EACAT).
- for the first time that the entity requests digital certificates, in which case it generally would not have any digital certificate to perform the request process through electronic media

4.1.1. Legitimacy of a request to issue

In accordance with the provisions of Certification General Policy related to infrastructure certificates issue, corporate and personal certificates, and device certificate requests.

4.1.2. Registration procedure; responsibilities

Not applicable.

4.2. Certification request procedure

4.2.1. General requirements for all certificates

The regular procedure for request of digital certificates is as follows:

1. Delivery of Subscriber Form

For a Public Sector of Catalonia entity to be able to request certificates, it must have previously sent the Fitxa del Subscriptor - correctly completed - to Consorci AOC. By this means, the Consorci AOC can register the entity accordingly in the management system and configure the necessary authorisations for the personnel indicated by the entity.

Usually this delivery shall be done by means of electronic media when all the roles that interact with the request process (applicant, certifier and service responsible) have digital certificates.

Alternatively, it is possible to issue the request (according to the reasons described in section *4.1 Request for certificate issue)* via the following alternative procedure:

- downloading the Subscriber Form from the Consorci AOC web
- delivery of the Card (correctly completed and digitally signed) to scd@aoc.cat; or (correctly completed and signed by hand) by postal mail to the address indicated in section *1.5.2 Contact details of the organization*.

This document will be delivered attached to the first certificates request, or when it is necessary to update the contained information.

2. Obtaining certificates

Completed requests made through electronic media must be digitally signed by the applicant, and where it is necessary to attach a data certificate, this will need to be digitally signed by the certifier:

- firstly when the applicant signs the request, the system sends automatically an email to the entity certifier warning him/her to verify the certificate request data.
- the certifier being the entity person who has the capacity to justify the certificate holder data which needs to be issued (for example, the secretary, the HR responsible, etc.) The entity certifier opens the request, verifies the data, digitally signs then ends the request process
- Once the request process has ended, the entity output register entry and the T-CAT Register Entity input register entry (the one which the entity belongs) are automatically updated

The EC-SECTORPUBLIC receives the request data and uploads it to the certificates generation application system, where it remains available for the corresponding Register Entity.

Once the Register Entity has generated the certificate, it is forwarded to the subscriber entity.

If the request is made through electronic media, it needs to follow the appropriate procedure:

- download of the request form and corresponding data certificate.
- delivery of the documents - correctly completed and digitally signed - to scd@aoc.cat; or delivery of the documents - correctly completed and signed by hand - by postal mail to the address indicated in section *1.5.2 Contact details of the organization.*

4.3. Certificate issue

Received requests are processed and validated.

If everything is correct, the request is sent to the Register Entity corresponding to the applicant entity. A message is then sent automatically to the applicant to inform regarding the process operation result in the positive or negative. If it is negative, the reasons are explained via referral to set error conditions.

4.3.1. EC-SECTORPUBLIC actions during the issuing process

Note: the procedures established in this section are also applicable for certificate renewals, due to the fact that a renewal implies a new certificate issue.

For each processed certificate request, the EC-SECTORPUBLIC shall act in accordance with the provisions in the Certification General Policy - section *4.3.1. Certification Entity Actions during issuing and renewal processes*.

4.3.2. Communicating the subscriber about the issue

EC-SECTORPUBLIC shall communicate with the applicant regarding request approval or rejection.

For approval cases, it shall also communicate (where appropriate) with the future key owner for which the certificate has been created, if there is a means available to do this.

4.4. Acceptance of certificate

For particular certificate profiles, EC-SECTORPUBLIC is responsible for the creation of a cryptographic key pair, while for all certificates remains responsible for generating the corresponding digital certificate.

For those certificate profiles which the key pair is generated and stored on cryptographic cards, EC-SECTORPUBLIC shall also be responsible for creating the corresponding PIN and PUK codes. These codes are sent directly to the key owner, usually via email but also through postal mail in a plain envelope in certain circumstances. The key owner is be able to recover these codes anytime through the telematic application.

At the same time, the card containing the requested certificate is sent through postal mail to the inner register entity of the subscriber entity.

EC-SECTORPUBLIC shall generate the certificate delivery and acceptance form for the key owner, where the described contents of the Certification General Policy are indicated.

4.4.1. Responsibilities of the Subscriber Body

4.4.1.1. For personal certificates

EC-SECTORPUBLIC is able to delegate to subscriber bodies (specifically to the responsible) some of its responsibilities regarding to the delivery and acceptance process of the digital certificates that it issues.

Specifically, the register entity responsible shall:

- inform the key owner of its obligations and responsibilities regarding to the certificate
- require the key owner to acknowledge receipt of the certificate, and of the corresponding cryptographic device (when applicable), as well as acceptance of these elements through signing the certificate delivery and acceptance form.
- For those profiles which require cryptographic card, deliver it to the key owner in person, once the key owner has signed the certificate delivery and acceptance form, as well as a copy of this form.

4.4.1.2. For device certificates

Device certificates shall be delivered by means of a file that the responsible subscriber entity must download.

4.4.2. Conduct which constitutes the certificate acceptance

The certificate is confirmed accepted through the key owner signature of the certificate delivery and acceptance form.

The possibility of accepting the certificate by means of a telematic mechanism that activates the certificate may also be considered.

4.4.3. Publication of the certificate

In accordance with the provisions of Certification General Policy.

4.4.4. Notifying the issue to third parties

Not applicable.

4.5. Use of the key pair and the certificate

4.5.1. Use for key owners

In accordance with the provisions of Certification General Policy.

4.5.2. Use for third party that trusts certificates

In accordance with the provisions of Certification General Policy.

4.6. Certificate renewal without keys renewal

Certificate renewal without keys renewal is not allowed.

4.7. Certificate renewal with keys renewal

In accordance with the provisions of Certification General Policy.

4.8. Telematic renewal

In accordance with the provisions of Certificate General Policy.

4.9. Modification of certificates

In accordance with the provisions of Certification General Policy.

Additionally and in particular circumstances (such as organizational changes, at the beginning of a new legislature, when some departments disappear and their functions are integrated in other departments, or just name changes), and in a transitory way, the non identifying data about the key owner that is recorded in the certificate (like email address, department, etc.) may not adapt to the new circumstances. In these cases, the organization shall plan the certificate renewal for its users. This can be delayed due to economic or organizational reasons, without being breach of the assigned responsibility.

4.10. Revocation and suspension of certificates

4.10.1. Causes of certificates revocation

In accordance with the provisions of Certification General Policy.

4.10.2. Legitimation for requesting a revocation

In accordance with the provisions of Certification General Policy.

4.10.3. Procedures for revocation request

The revocation request must be processed through telematic media. It shall be sent via signed email, or via certified postal mail in exceptional moments. It must to contain enough information to reasonably identify - under EC-SECTORPUBLIC criteria - the certificate that is requested for revocation, and the authenticity and authority of the applicant.

The supplied information needs to contain the detail contacts for the key owner (including National Id Document or equivalent), data regarding the revocation applicant entity, the certificate series number, plus current date and the reason for revocation to be requested.

The Register Entity may be asked for more information in order to complete this procedure.

The Register Entity should collect the necessary information and register the revocation request.

Register Entities should manage the revocation requests within regular office hours. Outside of these hours, when revocation of a certificate is urgent, a precautionary suspension can be requested through phone call to User Service Center of the Consorci AOC, which is available 24x365.

The suspension is forbidden for the following device certificates, being able to be only revoked:

- Device certificates SSL
- Device certificates SSL EV
- Mid-level electronic office certificate

Revocation action is made by one of the operators of the Register Entity, by accessing the web application and authenticating through an operator digital certificate (CIPISQ) issued by EC-SECTORPUBLIC.

Once the status change has been registered in the EC-SECTORPUBLIC system, a new Certificate Revocation List (LCR or CRL) is published, and the reference to this certificate shall be documented there.

The subscriber, and the key owner if applicable, are informed about the change on the certificate status, according to article 10.2 of Spanish Law of electronic signature.

4.10.4. Term time for revocation request

In accordance with the provisions of Certification General Policy.

4.10.5. Maximum term for revocation request process

In accordance with the provisions of Certification General Policy.

4.10.6. Obligation to consult information related to certificate revocation

In accordance with the provisions of Certification General Policy.

4.10.7. Issue frequency of the Certificate Revocation List

In accordance with the provisions of Certification General Policy.

4.10.8. Maximum period for Certificate Revocation List publication

In accordance with the provisions of Certification General Policy.

4.10.9. Availability of certificate status check services

In accordance with the provisions of Certification General Policy.

4.10.10. Obligation to consult information regarding certificate status check services

In accordance with the provisions of Certification General Policy.

4.10.11. Other forms of certificate revocation information

Without additional stipulation.

4.10.12. Special requirements for private key security breach cases

In accordance with the provisions of Certification General Policy.

4.10.13. Causes of certificate suspension

In accordance with the provisions of Certification General Policy.

4.10.14. Effect of certificate suspension

In accordance with the provisions of Certification General Policy.

4.10.15. Authorisation to request a suspension

In accordance with the provisions of Certification General Policy regarding to corporate certificate suspension.

4.10.16. Procedures of suspension request

In accordance with the provisions of Certification General Policy.

4.10.17. Maximum period for suspension

In accordance with the provisions of Certification General Policy.

4.10.18. Enabling a suspended certificate

In accordance with the provisions of Certification General Policy.

4.11. Certificate status check services

4.11.1. Operational features of the services

CRLs are published on the Consorci AOC website, and via the URLs indicated on the issued certificates.

Additionally, the verifiers shall be able to enquire on the published certificates in the E-SECTORPUBLIC directory.

4.11.2. Availability of the services

In accordance with the provisions of Certification General Policy.

4.11.3. Other functions of the services

Without additional stipulation.

4.12. End of the subscription

In accordance with the provisions of Certification General Policy.

4.13. Keys deposit and recovery

4.13.1. Policy and practices of keys deposit and recovery

There is no key recovery for certificates issued by EC-SECTORPUBLIC.

4.13.2. Policy and practices of session keys encapsulation and recovery

Without additional stipulation.

4.14. SSL-like certificates issues

To notify any concern related with the usage, correctness, security or other regarding any kind of website authentication or SSL certificate issued by the Responsible Organization, that is:

- Device certificates SSL,
- Device certificates SSL EV,
- Mid-level electronic office certificate,

please contact to the Contact details of the organization or the following electronic address:

incident_pki@aoc.cat,

providing, if possible:

1. Date and time
2. Certificate serial number
3. URL at you are trying to access to
4. IP address from you are trying to access to the above URL

5. Controls of physical, management and operation security

5.1. Control of physical security

In accordance with the provisions of Certification General Policy.

5.1.1. Location and construction of the facilities

In accordance with the provisions of Certification General Policy.

5.1.2. Physical access

In accordance with the provisions of Certification General Policy.

5.1.3. Electricity and air conditioner

In accordance with the provisions of Certification General Policy.

5.1.4. Water exposure

In accordance with the provisions of Certification General Policy.

5.1.5. Fire warning and protection

In accordance with the provisions of Certification General Policy.

5.1.6. Supports store

In accordance with the provisions of Certification General Policy.

5.1.7. Waste management

In accordance with the provisions of Certification General Policy.

5.1.8. Secure offsite copy

In accordance with the provisions of Certification General Policy.

5.2. Procedure controls

EC-SECTORPUBLIC guarantees that its systems operate in a secure way, by establishing and implementing procedures for the related functions that affect its service provision..

EC-SECTORPUBLIC personnel execute the administrative and management procedures according to the EC-SECTORPUBLIC security policy. This security policy offers support to roles with different privileges..

5.2.1. Reliable functions

In accordance with the provisions of Certification General Policy.

Reliable functions and obligations are described within section 5.3 of this document.

5.2.2. Number of persons per task

In accordance with the provisions of Certification General Policy.

5.2.3. Identification and authentication for each function

In accordance with the provisions of Certification General Policy.

5.2.4. Roles which require tasks separation

In accordance with the provisions of Certification General Policy.

5.3. Personnel controls

EC-SECTORPUBLIC considers the following aspects:

- Information confidentiality is maintained via available means and by keeping an appropriate attitude for the development of its functions, while outside of the work environment it is maintained by managing all aspects of infrastructures security.
- Being diligent and responsible with the treatment, maintenance and custody of the assets identified in the policy, within security plans or within this document.
- Non-public information shall not be revealed outside of the infrastructure. It is also not allowed to remove information media for sharing with lower security levels.
- Any incident which is considered to affect infrastructure security or to limit the service quality, must be reported to Security Responsible at the earliest opportunity.
- Infrastructure assets shall be used for the purposes for which they have been mandated.
- It is required to have manuals and guidelines for the system users that allow them to develop their functions correctly.
- Written documentation that indicates the functions and security measures to which the user is subjected, is required
- The security responsible ensures that the above referred documentation is supplied, and provides area responsible contacts with all the necessary information.
- No software or hardware that have not been specifically authorised in writing by the IT responsible, shall be installed.
- Intentional access, deletion or modification of information not designated for that person or professional profile, is not permitted.

Personnel bound by these regulations:

- Digital Certification Service Responsible

- EC-SECTORPUBLIC Responsible
- Security Responsible
- Operations Responsible
- Key Ceremony Operator
- administration, operation and exploitation Technical Team
- Network Administrators
- Register Entity Operators

In addition, regulation compliance extends to the following personnel of Consorci AOC who:

- submit certificate requests
- approve and validate certificate requests
- submit certificate generation / customisation
- guard keys or cryptographic tokens
- guard the keys or secure combinations to access the operation room
- retain access to classified information
- communications and operations personnel
- are security personnel (physical and logical) involved in the operation
- are the service responsible

5.3.1. Record, qualification, experience and authorisation requirements

In accordance with the provisions of Certification General Policy.

5.3.2. Training requirements

In accordance with the provisions of Certification General Policy.

In addition, Consorci AOC provides all the personnel involved in EC-SECTORPUBLIC Register Entities operations with appropriate information, including work and security procedures.

Periodic training on security rules, contingency plan and incident management is also given to internal personnel.

5.3.3. Requirement for and frequency of training update

In accordance with the provisions of Certification General Policy.

5.3.4. Sequence and frequency of job rotation

Without additional stipulation.

5.3.5. Penalties for unauthorised actions

In accordance with the provisions of Certification General Policy.

5.3.6. Requirements for hiring personnel

In accordance with the provisions of Certification General Policy.

5.3.7. Provision of documentation to personnel

In accordance with the provisions of Certification General Policy.

5.4. Procedures for security audit

5.4.1. Types of registered events

In accordance with the provisions of Certification General Policy.

5.4.2. Treatment frequency of audit registers

In accordance with the provisions of Certification General Policy.

5.4.3. Preservation period of audit registers

In accordance with the provisions of Certification General Policy.

5.4.4. Protection of audit registers

In accordance with the provisions of Certification General Policy.

5.4.5. Procedures for maintaining secure copies

In accordance with the provisions of Certification General Policy.

The following points have been instituted in order to correctly preserve secure copies:

- Materials are kept in fire-resistant cabinets
- Only authorised personnel can access to secure copies
- The copies are identified

- If a material that has already contained a secure copy (USB, DVD's…) needs to be reused, it is necessary to make sure that the data is completely deleted and impossible to recover.
- Secure copies removal outside Register Entity need to be specifically authorised, via submission of an appropriate request form and noting the details in the register book.
- It is intended that secure copies are deposited periodically outside of the Register Entity.

5.4.6. Location of accumulation systems of audit registers

In accordance with the provisions of Certification General Policy.

5.4.7. Notification of audit events to the event originator

In accordance with the provisions of Certification General Policy.

5.4.8. Analysis of security vulnerabilities

In accordance with the provisions of Certification General Policy.

5.5. Archive of informations

In accordance with the provisions of Certification General Policy.

5.5.1. Types of registered events

EC-SECTORPUBLIC maintains a register of all the events that occur during a certificate life cycle, including its renewal.

EC-SECTORPUBLIC registers the following points:

- Original documents:
  - Certificates request form
  - Data certificate
  - Delivery form for certificates subscriber

EC-SECTORPUBLIC maintains the following in regard of Extended Validation certificates:

- *LOG* and audit trail
- Documentation regarding to requests, verifications and revocations of Extended Validation certificates.

5.5.2. Register preservation period

L'EC-SECTORPUBLIC maintains the registers specified in section 5.5.1 during a 15 year retention period, initiated from the time of certificate dispatch.

EC-SECTORPUBLIC maintains the registers specified in section 5.5.1 regarding to Extended Validation certificates for 7 year retention period, initiated from the time of certificate dispatch.

5.5.3. Archive protection

In accordance with the provisions of Certification General Policy.

5.5.4. Support copy procedures

A communication technical worker from Consorci AOC is responsible for making secure copies of logic access logs to LRA operating system.

Secure copies are created on a monthly basis and stored as CD copies. These CDs are kept in a safety deposit box in the same room.

5.5.5. Requirements for date and hour seal

In accordance with the provisions of Certification General Policy.

5.5.6. Location of archive system

EC-SECTORPUBLIC has a storage system for archive data outside of its own facilities, as specified in section 5.1.8.

5.5.7. Procedures for obtaining and verifying archive information

In accordance with the provisions of Certification General Policy.

5.6. Keys renewal

l'EC-SECTORPUBLIC renewed certificates are communicated to end users through their publication in the section Servei SCD of the Consorci AOC web.

5.7. Keys security breach and disaster recovery

5.7.1. Procedures for incident and security breach management

L'EC-SECTORPUBLIC establishes the procedures that apply to incident management affecting keys, including and especially for key security breaches.

5.7.2. Resources, applications or data corruption

When a resource, application or data corruption event occurs, EC-SECTORPUBLIC initiates the necessary process management activities according to the Security Plan, Emergency Plan and Audit Plan documents, in order to ensure that affected systems come return to normal operations.

5.7.3. Security breach of entity private key

Business Continuity Plan of EC-SECTORPUBLIC (or disaster recovery plan) considers the security breach of private key, or the suspicion of security breach, as a disaster.

In security breach cases, EC-SECTORPUBLIC:

- Informs all the subscribers and verifiers about the security breach
- Indicates that the certificates and the information about its delivery revocation status using the EC-SECTORPUBIC are now valid and in effect.

5.7.4. Disaster on the facilities

EC-SECTORPUBLIC develops, keeps, proves, and if necessary executes, an emergency plan for disaster cases on the facilities, either if it is due to natural causes or it is caused by human error. This plan indicates how the Information Systems shall be restored. Disaster recovery systems location has the security physical protections that are described in the Security Plan.

EC-SECTORPUBLIC is able to restore PKI normal operation within the 24 hours following the disaster. It is possible, at least, to execute the following actions:

- Certificates revocation
- Publication of revocation information

The disaster recovery database used by EC-SECTORPUBLIC is synchronised with the production database, within the temporary limits that are specified in the Security Plan. The recovery disaster equipment has the physical security measures that are described in the Security Plan.

5.8. Service end

5.8.1. EC-SECTORPUBLIC

In accordance with the provisions of Certification General Policy.

5.8.2. Register Entities

Register Entities shall diligently preserve and guard all the generated information in its activity as a Register Entity during a 15 year retention period after the end of the activities related to the Register Entity.

6. Technical Security Controls

EC-SECTORPUBLIC uses reliable systems and products that are protected from all alterations and guarantee technical and cryptographic security within the certification processes which they provide support.

6.1. Key pair generation and installation

6.1.1. Key pair generation

6.1.1.1. Requirements for all the certificates

The key pair can be generated for the future key owner or the Register Entity.

6.1.1.2. Information for CPI, CPSQ, CPPI, CPPSQ and CPRISQ certificates

Public and private keys for CPI, CPSQ, CPPI, CPPSQ and CPRISQ certificates are generated by the Consorci AOC via qualified electronic signature creation device.

6.1.1.3. Information for CPISA certificates

Consorci AOC can generate public and private keys for CPISA certificates and send them to the key owner in a secure way. They can also be generated by the future key owner, who shall send the corresponding private key possession proof (PKCS#10) to EC-SECTORPUBLIC.

6.1.1.4. Information for CDS-1, CDS-1 EV, CDS-1 SENM, CDA-1, CDA-1 SENM certificates

Key pair of CDS-1, CDS-1 EV, CDS-1 SENM, CDA-1, CDA-1 SENM certificates are generated by the certificate applicant entity, the subscriber, who shall send the corresponding private key possession proof (PKCS#10) to EC-SECTORPUBLIC.

6.1.2. Delivery of private key to the subscriber

6.1.2.1. In accordance with the provisions of Certification General Policy.

6.1.3. Delivery of public key to the certificate issuer

In accordance with the provisions of Certification General Policy.

6.1.4. Distribution of the Certification Service Provider public key

EC-SECTORPUBLIC key and the keys of Certification Entities that are one level below in the certification public hierarchy of Catalonia, are communicated to the verifiers, guaranteeing key integrity and authenticating the origin.

EC-SECTORPUBLIC public key is published in the EC-SECTORPUBLIC directory in the form of a CIC certificate signed by EC-ACC. Users can access the directory to obtain the EC-SECTORPUBLIC public keys.

This certificate is also published in the Consorci AOC web.

Additionally, in S/MIME applications, the data message contains a certificate chain, including CIC certificates, with public keys of the Certification Entities of the hierarchy (EC-SECTORPUBLIC and EC-ACC in this case), that are distributed to users this way.

6.1.5. Key measures

All EC-SECTORPUBLIC certificate keys are minimum 2.048 bits.

6.1.6. Generation of public key parameters

Without additional stipulation.

6.1.7. Quality verification of public key parameters

In accordance with the provisions of Certification General Policy.

6.1.8. Generation of keys in IT applications or pieces of equipment

In accordance with the provisions of Certification General Policy.

6.1.9. Key use purposes

L'EC-SECTORPUBLIC includes the KeyUsage extension in all certificates, indicating the expected and allowed uses of the corresponding private keys.

6.2. Protection of private key

6.2.1. Protection modules of private key

6.2.1.1. Cryptographic module standards

In accordance with the provisions of Certification General Policy.

6.2.1.2. Life cycle of cards with integrated circuit

In accordance with the provisions of Certification General Policy.

6.2.2. Control for more than one person (n de m) over private key

In accordance with the provisions of Certification General Policy.

6.2.3. Private key deposit

In accordance with the provisions of Certification General Policy.

6.2.4. Secure copy of private key

In accordance with the provisions of Certification General Policy.

6.2.5. Private key archive

In accordance with the provisions of Certification General Policy.

6.2.6. Insertion of private key into cryptographic module

In accordance with the provisions of Certification General Policy.

6.2.7. Storage of private key in the cryptographic module

In accordance with the provisions of Certification General Policy

6.2.8. Activation method of private key

At least two persons are required to activate the EC-SECTORPUBLIC private key.

For personal and entity certificates, the private key of the key owner activates through PIN code insertion in the smart card.

6.2.9. Private key deactivation method

In accordance with the provisions of Certification General Policy.

6.2.10. Private key destruction method

In accordance with the provisions of Certification General Policy.

6.2.11. Classification of cryptographic modules

In accordance with the provisions of Certification General Policy.

6.3. Other management aspects of the key pair

6.3.1. Public key archive

EC-SECTORPUBLIC archives public keys in accordance with the provisions of section 6.2.

6.3.2. Use period of public and private keys

In accordance with the provisions of Certification General Policy.

6.4. Activation data

6.4.1. Generation and installation of activation data

In accordance with the provisions of Certification General Policy.

6.4.2. Protection of activation data

In accordance with the provisions of Certification General Policy.

6.4.3. Other aspects of activation data

Without additional stipulation.

6.5. IT security controls

6.5.1. Specific technical requirements for IT security

In accordance with the provisions of Certification General Policy.

6.5.2. Evaluation of IT security level

The certification authority application, by which EC-SECTORPUBLIC operates (EJBCA Enterprise Edition) is reliable, due to achievement of Common Criteria EAL4+ certification compliance.

6.6. Life cycle technical controls

6.6.1. System development controls

In accordance with the provisions of Certification General Policy.

6.6.2. Security management controls

In accordance with the provisions of Certification General Policy..

In addition, EC-SECTORPUBLIC guarantees that functions of cryptographic modules operation management are sufficiently secure; in particular there are instructions for:

a. operating the modules in a correct and safe way
b. installing those modules that minimise system failure risk
c. protecting those modules against virus and malware in order to guarantee the integrity and validity of the information they process

6.6.3. Evaluation of life cycle security level

Without additional stipulation.

6.7. Network security controls

It is guaranteed that the access to EC-SECTORPUBLIC from different networks is restricted to duly authorised individuals. In particular:

- In order to protect the internal network against third parties accessible external domains, some controls are implemented (for example firewalls). Such firewalls are configured to avoid accesses and protocols that are not necessary for IC-SECTORPUBLIC operations.

- Sensitive data (including subscriber register data) are protected when they are exchanged through non-secure networks.
- It is guaranteed that network local components (like routers) are located in secure environments. Periodical audit of such configurations ensure this guarantee.

6.8. Time stamp

Without additional stipulation.

7. Certificate profiles and certificate revocation lists

7.1. Certificate profile

In accordance with the provisions of Certification General Policy.

Documents which describe the different certificate profiles that EC-SECTORPUBLIC dispatches, are published in the Consorci AOC web.

7.2. Certificate revocation list profile

In accordance with the provisions of Certification General Policy.

8. Conformity audit

EC-SECTORPUBLIC will periodically conduct conformity audits designed for proving compliance with those security and operation requirements for being a part of the certification public hierarchy of Catalonia.

EC-SECTORPUBLIC may delegate the audit execution to a third party hired by Consorci AOC. In such cases, EC-SECTORPUBLIC will entirely cooperate with the third party personnel assigned to conducting the investigation.

8.1. Frequency of conformity audit

In accordance with the provisions of Certification General Policy.

8.2. Identification and qualification of the auditor

EC-SECTORPUBLIC will engage with external independent auditors in order to conduct the annual conformity audit. Prospective auditors must demonstrate experience on IT security, Information Systems security, and conformity audits on Certification Authorities and related elements.

8.3. Relation between auditor and audited entity

External conformity audits executed by third parties are conducted by entities that are independent form EC-SECTORPUBLIC.

8.4. List of elements to be audited

In accordance with the provisions of Certification General Policy.

8.5. Required actions resulting from lack of conformity

In accordance with the provisions of Certification General Policy.

8.6. Treatment of audit reports

Audit result reports shall be delivered to Consorci AOC (since it is the Certification Service Provider) within a period of maximum 15 days from the audit execution, for its evaluation and diligent management.

9. Commercial and legal requirements

9.1. Rates

9.1.1. Certificate issuing and renewal rate

Consorci AOC establishes the rates that EC-SECTORPUBLIC applies in its services provision. Rates can be consulted in the Consorci AOC web.

9.1.2. Certificate access rate

It is not possible to establish a certificate access rate.

9.1.3. Certificate status access information rate

It is not possible to establish a certificate status access information rate.

9.1.4. Other services rate

Without additional stipulation.

9.1.5. Reimbursement policy

Consorci AOC shall not make reimbursements. For defective product cases, they shall be replaced by other in good conditions.

9.2. Financial capacity

9.2.1. Civil liability insurance

Consorci AOC has a guarantee of coverage enough for its civil liability, under the terms provided in article 20.2 of Spanish Law 59/2003, dated 19th December, except when it is exempt of this obligation by Law. This insurance covers the activities of Consorci AOC as a provider of certification services.

9.2.2. Other assets

Without additional stipulation.

9.2.3. Insurance cover for subscribers and third parties who trust certificates

For cases of incorrect or unauthorised use of certificates, Consorci AOC (or EC-SECTORPUBLIC) shall not act as a trustee in front of subscribers and third parties, who shall address against the offender of certificate use conditions established by Consorci AOC (or EC-SECTORPUBLIC).

9.3. Confidentiality

9.3.1. Confidential informations

In accordance with the provisions of Certification General Policy.

9.3.2. No confidential informations

In accordance with the provisions of Certification General Policy.

9.3.3. Responsibility for protection of confidential information

In accordance with the provisions of Certification General Policy.

9.4. Personal data protection

9.4.1. Personal Data Protection Policy

In accordance with the provisions of Certification General Policy.

9.4.2. Personal Data not available for third parties

In accordance with the provisions of Certification General Policy.

9.4.3. Personal Data available for third parties

In accordance with the provisions of Certification General Policy.

9.4.4. Responsibility corresponding to personal data protection

In accordance with the provisions of Certification General Policy.

9.4.5. Incident management related to personal data

In accordance with the provisions of Certification General Policy.

9.4.6. Consent for personal data treatment

In accordance with the provisions of Certification General Policy.

9.4.7. Personal data communication

In accordance with the provisions of Certification General Policy.

9.5. Intellectual property rights

9.5.1. Certificates and revocation information property

In accordance with the provisions of Certification General Policy.

9.5.2. Certification Policy and Certification Practice Statement property

In accordance with the provisions of Certification General Policy.

9.5.3. Property of information related to names

In accordance with the provisions of Certification General Policy.

9.5.4. Keys property

In accordance with the provisions of Certification General Policy.

9.6. Obligations and civil liability

9.6.1. Certification Entities

9.6.1.1. EC-SECTORPUBLIC general obligations

In accordance with the provisions of Certification General Policy.

9.6.1.2. Specific requirements for personal certificates

In accordance with the provisions of Certification General Policy.

9.6.1.3. Additional information for CDS-1, CDS-1 EV, and CDS-1 electronic office

In accordance with the provisions of Certification General Policy.

The established obligations are exercised within the policies, practices and general rules framework of the certification public hierarchy of Catalonia.

9.6.1.4. Guarantees offered to subscribers and verifiers

In accordance with the provisions of Certification General Policy.

9.6.2. Obligations and other commitments of Register Entities

9.6.2.1. Obligations and other commitments

In accordance with the provisions of Certification General Policy. Apart from the obligation of storing the certificate delivery forms during a 15 year retention period, which is assumed by the subscriber entities of corporate certificates that EC-SECTORPUBLIC issues.

Regarding the number of operators that the register authority needs to designate: for EC-SECTORPUBLIC shall be 4 or more of its employees.

9.6.3. Obligations and other commitments of the subscriber entities of corporate certificates issued by EC-SECTORPUBLIC

Subscriber entities of certificates issued by EC-SECTORPUBLIC undertake to storage the certificate delivery forms during a 15 year retention period.

These registers shall be available for the Affiliated Certification Entity.

9.6.4. Guarantees offered to subscriber and verifiers

9.6.4.1. Guarantee of Consorci AOC for digital certification services

In accordance with the provisions of Certification General Policy.

9.6.4.2. Exclusion of the guarantee

In accordance with the provisions of Certification General Policy.

9.6.5. Subscribers

9.6.5.1. Obligations and other commitments

9.6.5.1.1. Information for all types of certificate

In accordance with the provisions of Certification General Policy.

9.6.5.1.2. Specific information for qualified electronic signature certificates

In accordance with the provisions of Certification General Policy.

9.6.5.2. Guarantees offered to the subscriber

In accordance with the provisions of Certification General Policy.

9.6.5.3. Private key protection

In accordance with the provisions of Certification General Policy.

9.6.6. Verifiers

9.6.6.1. Obligations and other commitments

In accordance with the provisions of Certification General Policy.

9.6.6.2. Guarantees offered to the verifier

In accordance with the provisions of Certification General Policy.

9.6.7. Other participants

9.6.7.1. Directory obligations and guarantees

In accordance with the provisions of Certification General Policy.

9.6.7.2. Guarantees offered to the directory

EC-SECTORPUBLIC takes the civil responsability of the certification directory.

9.7. Guarantee disclaimer

9.7.1. Rejection of EC-SECTORPUBLIC guarantees

EC-SECTORPUBLIC may reject all service guarantees that are not linked to established obligations on Spanish Law 59/2003, dated 19th December, in particular including the guarantee of adaptation for a particular purpose or guarantee for certificate commercial use.

9.8. Limitations of Responsibility

9.8.1. EC-SECTORPUBLIC limitations of responsibility

Beyond the certification service providers limitations established in article 23 of Spanish Law 59/2003, dated 19th December, EC-SECTORPUBLIC limits its responsibility by restricting the certificate issuing and management service, and where appropriate, the subscriber key pair and cryptographic deposit service (of signature and signature verification as well as of encoding and decoding).

For particular types of certificates, EC-SECTORPUBLIC limits its responsibility through including certificate use limits and value limits for transactions that the certificate can be used for.

9.8.2. Fortuitous event and force majeure

EC-SECTORPUBLIC includes clauses to limit its responsibility in fortuitous events and force majeure cases, on legal instruments with subscribers.

9.9. Compensations

9.9.1. Subscriber indemnity clause

No subscriber indemnity clause shall be established.

9.9.2. Verifier indemnity clause

No verifier indemnity clause shall be established.

9.10. Term and end

9.10.1. Term

EC-SECTORPUBLIC establishes, in its legal instruments with the subscribers, a clause that determines the legal relation validity period in which EC-SECTORPUBLIC provides them certificates.

9.10.2. Term end

EC-SECTORPUBLIC establishes, in its legal instruments with the subscribers, a clause that determines the consequences of ending the legal relation by which EC-SECTORPUBLIC provides them certificates.

9.10.3. Survival

In accordance with the provisions of Certification General Policy.

9.11. Notifications

In accordance with the provisions of Certification General Policy.

9.12. Modifications

9.12.1. Modification procedures

In accordance with the provisions of Certification General Policy.

9.12.2. Term and mechanics for notifications

Modifications in this document shall be approved by the Consorci AOC, in accordance with the provisions of section 1.5.

9.12.3. Circumstances where OID must be changed

Without additional stipulation.

9.13. Conflicts resolution

9.13.1. Conflicts extrajudicial resolution

In accordance with the provisions of Certification General Policy.

9.13.2. Competent jurisdiction

In accordance with the provisions of Certification General Policy.

9.14. Applicable law

In accordance with the provisions of Certification General Policy.

9.15. Conformity with applicable law

In accordance with the provisions of Certification General Policy.

9.16. Diverse clauses

9.16.1. Entire agreement

In accordance with the provisions of Certification General Policy.

9.16.2. Subrogation

In accordance with the provisions of Certification General Policy.

9.16.3. Divisibility

In accordance with the provisions of Certification General Policy.

9.16.4. Applications

Without additional stipulation.

9.16.5. Other clauses

Without additional stipulation.

10. APPENDIX – Document control

Project:	**Creation report of EC-SECTORPUBLIC CPS document**
Destination entity:	**SCD Service - Consorci AOC**
Reference code:	**Review 1st trimester 2018**
Version:	**Initial version**
Edition date:	**09/05/2018**

Version	Parts that change	Change description	Change author	Change date
1.0	All the document	Initial writing of Certification Practices Statement of EC-SECTORPUBLIC	CATCert Service of Consorci AOC	20/01/2016
2.0	All the document	Adaptation to eIDAS requirements	CATCert Service of Consorci AOC	09/05/2018