Consorci
Administració Oberta
de Catalunya

# Certification Policy for

# Devices and Infrastructure

# Consorci AOC

| | |
|---|---|
| Reference: | PC DEVICES AND INFRASTRUCTURE |
| Version: | 6.3 |
| Date: | 27/01/2021 |
| OID: | 1.3.6.1.4.1.15096.1.3.2.1.3 |

The valid original version of this document can be found in the electronic format published by Consorci AOC on its website and is accessible at this URL: https://www.aoc.cat/catcert/regulacio/

**Version history**

| Version | Summary of amendments | Date |
|---|---|---|
| 5.0 | Adaptation to eIDAS | 9/05/2018 |
| 6.0 | Creation of a new specific Certification Policy for Devices and Infrastructures based on the prior general policy. It is numbered as "Version 6.0" for the purposes of documentary management and continuance of the prior general policy. | 26/07/2018 |
| 6.1 | ● Annual review of the documentation, post eIDAS audit.<br>● "3.1. Valid term of the certificate": modified validity of the application certificates to 4 years.<br>● Created "*4.3.5. CAA validations*" where the validations carried out on CAA records for SSL and EV certificates are explained. | 24/07/2019 |
| 6.2 | ● Adaptation to the requirements of version 2.7 of the Mozilla Root Store Policy. | 31/03/2020 |
| 6.3 | ● Policy review<br>● Adaptation to Law 6/2020, of November 11, regulating certain aspects of electronic trust services | 27/01/2021 |

# Contents

# 1. Introduction

## 1.1. Presentation and scope of application

The device and infrastructure certificates referred to in this Certification Policy (CP) are issued by Consorci AOC for use by all entities that make up the public sector of Catalonia under the terms of Article 2.1 of the Law 29/2010, of August 3, on the use of electronic media to the public sector of Catalonia, in accordance with the provisions of art. 7 of Law 29/2010 and art. 7 of the Statutes of the Consorci AOC approved by Agreement GOV / 43/2015, of March 24, which approves the modification of the statutes of certain consortiums, with majority participation of the Generalitat of Catalonia.

Device and infrastructure certificates are characterized by the fact that the private key holder is a computer device that carries out the signature and encryption transactions automatically, under the responsibility of a natural or legal person (referred to as the Subscriber or Certificate Holder).

This PC was drawn up according to Standard RFC 3647 of the IETF. The certificates issued pursuant to this CP meet the requirements established in EU Regulation (EU) 910/2014, of the European Parliament and of the Council, of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 / EC (Regulation (EU) Nº 910/2014).

This document specifies the Certification Policy for the following certificate types:

- Application Certificate (*Dispositiu aplicació*)
- Advanced Electronic Seal Certificate (*Segell nivell mig*)
- Electronic Office Certificate (*Seu-e nivell mig*)
- Secure Server Certificate (*Dispositiu SSL*)
- Secure Server Certificate Extended Validation (*Dispositiu SSL EV*)
- Qualified Time Stamping Certificate *(Segell de temps)*

This PC is subject to Consorci AOC's Certification Practices Statement (CPS), which it includes by reference.

## 1.2. Name of the document and identification

### 1.2.1. Identification of this document

| | |
|---|---|
| **Name:** | PC Devices and Infrastructure |
| **Version:** | 6.3 |
| **Description** | Certification Policy for Devices and Infrastructure |
| **Date of issue:** | 27/01/2021 |
| **OID:** | 1.3.6.1.4.1.15096.1.3.2.1.3 |
| **Location:** | https://www.aoc.cat/catcert/regulacio |

### 1.2.2. Identification of certification policies for each certificate type

| Certificate type | OID |
|---|---|
| Application certificate (*Dispositiu aplicació*) | 1.3.6.1.4.1.15096.1.3.2.91.1 |
| Advanced Electronic Seal Certificate (*Segell nivell mig*) | 1.3.6.1.4.1.15096.1.3.2.6.2 |
| Electronic Office Certificate (*Seu-e nivell mig*) | 1.3.6.1.4.1.15096.1.3.2.5.2 |
| Secure Server Certificate (*Dispositiu SSL*) | 1.3.6.1.4.1.15096.1.3.2.51.1 |
| Secure Server Certificate Extended Validation (*Dispositiu SSL EV*) | 1.3.6.1.4.1.15096.1.3.2.51.2 |
| Qualified Time Stamping Certificate *(Segell de temps)* | 1.3.6.1.4.1.15096.1.3.2.111 |

The documents describing these certificate profiles are published on Consorci AOC's website.

# 2. Participating entities

## 2.1. Trust Service Providers (TSP)

The certificates issued pursuant to this Certification Policy are issued by Consorci AOC as the trust certification service provider through its subordinate CA (Certification Authority) "EC-SECTORPUBLIC".

## 2.2. Registration Authorities

The Registration Authorities are the natural and legal persons that assist the CSP in certain procedures and relations with the certificate subscribers and applicants, particularly the processes involving identification, registration and authentication of certificate subscribers and key holders.

Consorci AOC is responsible for the process that creates EC-SECTORPUBLIC registration authorities. It verifies that the Registration Authority has the necessary human and material resources; and that said authority has appointed and trained the staff that will be responsible for issuing the certificates (the so-called "operators" of the Registration Authority).

There are two types of EC-SECTORPUBLIC Registration Authorities:

1. Subscription entities, which are operated by a certificate subscriber entity.
2. Registration authorities, which collaborate with EC-SECTORPUBLIC the certificate issuance process.

To be registration authorities, the entities in question must design and implement the relevant technical, legal and security components and procedures, with regard to the lifecycle of the qualified devices used in the signature creation or, as the case may be, in the key creation; with regard to the lifecycle of the keys in support software; and with regard to the lifecycle of the certificates that they issue. These components and procedures shall be approved previously by Consorci AOC.

## 2.3. Final users

The final users are the persons that obtain and use the electronic certificates. Specifically, the following final users can be highlighted:

- The certificate applicants.

- The certificate subscribers.
- The key holders.
- Relying parties.

### 2.3.1. Certificate applicants

The following can be applicants of EC-SECTORPUBLIC certificates:

a) For corporate certificates: a person that has been authorized for such purposes by the future subscribing entity
b) A person authorized by the CSP – typically, Consorci AOC, acting by operation of law..

The authorization shall be formalized in a written document.

### 2.3.2. Certificate subscribers

Certificate subscribers are the institutions and the individuals or companies, under whose name the relevant certificate will be issued, as identified in the “Subject” field of the certificate.

The requirements that a subscriber must meet for each certificate type stipulated under this CP are the following:

### 2.3.3. Key holders

Key holders are individuals that have exclusive possession of the certified electronic seal or authentication keys, either to act in their own name and on their own behalf, or because they have been authorized to hold them by the subscriber.

The key holders or signatories are responsible for keeping the information necessary to create the signature or authentication associated with the electronic certificate, under their custody.
The Subscriber shall be responsible for any action taken by the key holders.

### 2.3.4. Relying parties

Relying parties (third parties that rely on the certificates) can be any person or organization that voluntarily relies on the certificates that are issued under any of Consorci AOC's certification hierarchies, described in the Certification Practice Statement.

The obligations and responsibilities of the Consorci AOC with third parties that voluntarily rely on the certificates shall be limited to those set out in this CP, in the CPS, in EU Regulation 910/2014 and in any other regulations that may be applicable.

The third parties that rely on these certificates must keep in mind these limitations with regard to use.

# 3. Characteristics of the certificates

## 3.1. Valid term for the certificate

The following electronic certificates issued under this Certification Policy shall be valid from their issuance date, provided that the relevant certificate has not been suspended or revoked:

- Application certificate (*Dispositiu aplicació*): 4 years.
- Advanced Electronic Seal Certificate (*Segell nivell mig*): 3 years.

The other certificates issued under the scope of this Certification Policy shall be valid for 2 years from the issuance date, provided that the relevant certificate has not been revoked:

## 3.2. Use of the certificates

This section lists the applications for which each type of certificate can be used, establishes restrictions, and prohibits certain uses of the certificates.

### 3.2.1. Typical use of the certificates

The certificates of Consorci AOC that are issued pursuant to this Certification Policy may be used for the following purposes:

| **Certificate type** | **Scope of application** |
|---|---|
| Application certificate (*Dispositiu aplicació*) | ● Authentication<br>● Electronic seal |
| Advanced Electronic Seal Certificate (*Segell nivell mig*) | ● Authentication<br>● Electronic seal |
| Electronic Office Certificate (*Seu-e nivell mig*) | ● Authentication<br>● Electronic seal |
| Secure Server Certificate (*Dispositiu SSL*) | ● Authentication |
| Secure Server Certificate Extended Validation (*Dispositiu SSL EV*) | ● Authentication |
| Qualified Time Stamping Certificate *(Segell de Temps)* | ● Authentication<br>● Electronic seal<br>● Time and date stamping certification |

### 3.2.2. Forbidden uses

The certificates may only be used within the limits expressly set out in this Certification Policy and in the CPS. Any other uses, except for those described therein, are expressly excluded from the contractual scope and are formally forbidden. Any illegal use of the certificates is expressly forbidden.

The certificates were not designed and are not destined or authorized for use or resale as devices to control dangerous situations, or for uses that require infallible actions, such as for the operation of nuclear installations, navigating systems, aerial communication, or weapon-control systems, where an error could imply death, personal injury or serious environmental damages.

The final user certificates cannot be used to sign public key certificates of any type, or to sign lists of certificate revocations.

The use of these certificates for document encryption is not recommended.

# 4. Operational procedures

## 4.1. Management of the Certification Policy

### 4.1.1. Organization that managers the specification

Consorci Administració Oberta de Catalunya – Consorci AOC

### 4.1.2. Contact information of the organization

Consorci Administració Oberta de Catalunya – Consorci AOC

Registered offices: Via Laietana, 26 – 08003 Barcelona

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

Website of Consorci AOC: https://www.aoc.cat/

Website of Consorci AOC's electronic certification service:

https://www.aoc.cat/catcert/

User Service Department: 900 90 50 90, or +34 93 272 25 01 for calls from outside the state, open 24/7.

Incidents with website authentication certificates: incident_pki@aoc.cat

## 4.2. Publication of information and certificate directory

### 4.2.1. Certificate directory

The certificate directory service is available 24 hours a day, 7 days a week. In the event an error arises that Consorci AOC cannot control, the latter shall make its best efforts to ensure the service is made available again and within the term set out in Section 5.7.4 of the CPS.

### 4.2.2. Publication of information

This Certification Policy is public and available on Consorci AOC's website (https://www.aoc.cat/catcert/regulacio/).

# 4.3. Operational features of the certificates' life cycle

## 4.3.1. Application for certificate issuance

Those public entities that wish to obtain a certificate under this Certification Policy can submit their application using the procedure established in the Manual, hung in the Subscriber Folder at https://www.aoc.cat/catcert/.

## 4.3.2. Legitimization to apply for a certificate

Only Public Administrations may request the Devices and Infrastructure Certificates that they need to perform their duties electronically, in accordance with the applicable regulations in force.

## 4.3.3. Certificate application processing

When a certificate application is received, the Certification Authority shall verify the information provided, according to the relevant section under this CP or the CPS.

If the information is incorrect, the Certification Authority must reject the application. If the information is correct, the Certification Authority will approve the application and allow the certificate to be issued.

The Certification Authority shall:

- Use a certificate-creation procedure that securely links the certificate with the registration information, including the certified public key.
- In the event that the Certification Authority generates the pair of keys, it shall use a certificate-creation procedure that is securely linked to the key-creation procedure so that the private key is delivered in a secure manner to the key holder.
- Protect the integrity of the registration information.
- Include the required information in the certificate.
- Guarantee the date and hour a certificate is issued.
- Use reliable systems and products that are protected against any alteration and which guarantee the technical and cryptographic security of the certification processes they support.
- Ensure that the certificate is issued by systems that protect against forgery and, if the Certification Authority generates private keys, that the systems ensure that keys are kept secret during the key-creation process.

*Nota*: The procedures established in this section are also applicable to certificate renewals, given that renewal implies issuing a new certificate.

## 4.3.4. Creation and implementation of activation keys

The Registration Authority's Agent shall validate the veracity and accuracy of the signatory's information and inform the Certification Authority thereof.

The Registration Authority's Agent shall validate the key holder's possession of the private information associated with electronic certificate to be issued.

Consorci AOC then provides the subscriber with the information to activate the signature-creation or authentication device on one hand and, on the other, it provides the subscriber with access to the device itself in a period of 3 (three) days.

## 4.3.5. Certification Authority Authorization (CAA) validations

Prior to the issuance of the SSL OV, SSL EV and Electronic Office certificates, the existence of CAA registration for each DNS name of the CN extensions and subjectAltName of the certificate is validated. In the event that the certificate is issued, the validation will be carried out before the time-to-live (TTL) of the CAA record.

The domain validation check is detailed in point 3.2.4 of the CPS.

The Consorci AOC processes the "issue" and "issuewild" tags.

The CAA registry that identifies domains for which the issuance is authorized by the Consorci AOC is "aoc.cat".

## 4.3.6. Certificate issuance

The Registry Authority's agent shall issue a certificate application using a standard form and send it to the Certification Authority.

The Certification Authority shall validate the integrity of the application and the fact that it was produced by an authorized Registration Authority agent. Once said validation takes place, the certificate shall be issued.

## 4.3.7. Notification of issuance to the subscriber

Consorci AOC shall notify the applicant indicating whether the certificate application submitted was approved or rejected.

If it is approved, Consorci AOC shall also notify the future key holder by email, if suitable, so they are informed that the certificate was issued, is available and regarding the way they may obtain it.

To obtain the certificate, the subscriber has to access the website indicated in the aforementioned email and follow the instructions set out therein to download the certificate.

### 4.3.8. Deliver and protection of the activation information

To provide maximum protection to the activation information, Consorci AOC undertakes to distribute the certificate elements via two different channels.

- Firstly, the Registration Authority's agent shall provide the key holder with access to the following material:
    - Holder's delivery sheet
    - Device with the certificates where appropriate, or software certificates
    - Software necessary to use the device
    - Certificate-delivery slips.
- Simultaneously, the activation-key holder will be sent the certificate's activation information by email.

Thus, the activation information is sent separately from the card and at different times

### 4.3.9. Certificate suspension

Suspension of web authentication certificates is not allowed, that is, the Electronic Office certificates and the secure server certificates. For the rest of the certificates collected in this CP, as detailed in the CPS.

### 4.3.10. Certificate revocation

According to the provisions of the CPS.

### 4.3.11. Certificate renewal

According to the provisions of the CPS.

### 4.3.12. Qualified Time Stamping Certificate

This guarantees the existence and integrity of the electronic file or correspondence at a certain date and time, using a reliable time source. The Qualified Time Stamping Certificates issued by Consorci AOC comply with the requirements set out in art. 42 of EU Regulation 910/2014.

Consorci AOC's time stamping service is described at https://www.aoc.cat and under the relevant policy, which is also hung on the same website.

## 4.4. Notification of problems with the website authentication certificates

To report any problem related to the use, accuracy or security of any website authentication certificate or Secure Server Certificate issued by the Consorci Administració Oberta de Catalunya, which is to say, regarding:

- Secure Server Certificate (*Dispositiu SSL*)
- Secure Server Certificate Extended Validation (*Dispositiu SSL EV*)
- Electronic Office Certificate (*Seu-e nivell mig*)

Please contact Consorci AOC using the organization's contact information or by sending an email to this address:

incident_pki@aoc.cat,

Providing the following therewith, if possible:

- Date and time.
- Certificate's serial number
- URL that is being accessed
- IP address from which you are trying to access the URL.

# 5. Profile of the certificates issued under this Certification Policy

The following certificate types are issued under this Certificate Policy:

| **Certificate type** | **OID** |
|---|---|
| Application certificate (*Dispositiu aplicació*) | 1.3.6.1.4.1.15096.1.3.2.91.1 |
| Advanced Electronic Seal Certificate (*Segell nivell mig*) | 1.3.6.1.4.1.15096.1.3.2.6.2 |
| Electronic Office Certificate (*Seu-e nivell mig*) | 1.3.6.1.4.1.15096.1.3.2.5.2 |
| Secure Server Certificate (*Dispositiu SSL*) | 1.3.6.1.4.1.15096.1.3.2.51.1 |
| Secure Server Certificate Extended Validation (*Dispositiu SSL EV*) | 1.3.6.1.4.1.15096.1.3.2.51.2 |
| Qualified Time Stamping Certificate *(Segell de Temps)* | 1.3.6.1.4.1.15096.1.3.2.111 |

The documents describing these certificate profiles are published on Consorci AOC website (https://www.aoc.cat/catcert/regulacio).