Consorci
Administració Oberta
de Catalunya

Certification Policy for Citizenship Certificates Consorci AOC

Reference:	CP CITIZENSHIP
Version:	6.1
Date:	24/07/2019
OID:	1.3.6.1.4.1.15096.1.3.2.1.1

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 Citizenship Certificates 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.	24/07/2019

Contents

1. Introduction

1.1. Presentation and scope of application

The electronic certificates referred to in this Certification Policy (CP) are **qualified certificates** issued by Consorci AOC to be used by natural persons that need to deal with entities that form part of the public sector in Catalonia. They are also **personal certificates**, given that that the holder of the private key and the certificate is a natural person.

This CP was drawn up according to Standard RFC 3647 of the IETF. The certificates issued pursuant to this CP meet the requirements established in Annex I of EU Regulation 910/2014.

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

- Qualified Citizenship Certificate (*idCAT certificat*) for electronic identification, creation, and use of "advanced electronic signatures".

This Certification Policy 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:	CP de Ciudadania
Version:	6.1
Description	Certification Policy for Qualified Citizenship Certificates
Date of issue:	24/07/2019
OID:	1.3.6.1.4.1.15096.1.3.2.1.1
Location:	https://www.aoc.cat/catcert/regulacio/

1.2.2. Identification of certification policies for each certificate type

Certificate type	**OID**

Qualified Citizenship Certificate (*idCAT certificat*)	1.3.6.1.4.1.15096.1.3.2.86.2

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 certification service provider through its subordinate CA (Certification Authority) "EC-CIUTADANIA".

2.2. Registration Authorities

The Registration Authorities are the natural and legal persons that assist the TSP 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-CIUTADANIA registration authorities. It verifies that the Registration Authority has the necessary human and material resources; and that said entity has appointed and trained the staff that will be responsible for issuing the certificates (the so-called "operators" of the Registration Authority).

2.3. Final Users

The Final Users are the persons that use the personal electronic certificates issued by EC-CIUTADANIA. 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 persons may be EC-CIUTADANIA certificate applicants:

a) Natural persons who, acting for and on their own behalf, will be future certificate subscribers.

b) Other persons authorized by the future Subscribers in writing (representatives).

2.3.2. Certificate subscribers

Certificate subscribers are the natural persons on behalf of whom the relevant certificate is issued and whose name appears in the "Subject" field of the certificate. They are entitled to use the certificate.

2.3.3. Key holders or signatories

The key holder or signatory is the natural person that creates the electronic signature.

For the purposes of this CP, the key holders or signatories are the Certificate Subscribers, as they are identified in the section above.

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. Certificate characteristics

3.1. Valid term for the certificates

The electronic certificates issued under this Certification Policy shall be valid for 4 (four) years from their issuance date, provided that the relevant certificate has not been suspended or revoked.

3.2. Use of the certificates

The idCAT advanced-signature certificates are qualified certificates, pursuant to the provisions of applicable laws. The idCAT certificates do not necessarily work with qualified devices for electronic-signature creation, according to said applicable laws. Although the advanced electronic signature is not directly like a written signature, such equalization can

arise under the case of the existence of an electronic signature contract or of a specific legal norm that reflects this equalization.

This section lists the applications for which the type of certificate mentioned herein 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**
Qualified Citizenship Certificate (*idCAT certificat*)	● Authentication ● Electronic signature

The certificates issued under this Policy can be used for the following purposes:

- **Identification of the Signatory**: The Signatory can authenticate their identity, vis-à-vis another party, by showing that their private key is associated to the public key contained in the Certificate. The Signatory may validly identify themself to any person by signing an email or any other type of information.

- **Integrity of the signed document**: The use of the Certificate guarantees the integrity of the signed document; that is to say, it guarantees that the document was not altered or modified after the Signatory executed it. The message received by the User relying on it is certified to be the same as the one issued by the Signatory.

- **Irrefutable origin**: This Certificate can also be used to guarantee that the Signatory undertakes a binding condition with the information related to the electronic signature; it provides sufficient evidence to demonstrate to who the related information belongs and the integrity thereof.

Furthermore, the certificates issued under this Policy may be used for the following:

- **Remote identification**, based on the presentation of the credentials.
- **Electronic authentication** for access-control systems.

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 manages 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

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

Web 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 to manage certificate suspensions.

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

An application is the first step for the Subscriber to obtain the certificates for their personal use.

Citizens that wish to obtain an idCAT certificate can do so in two ways:

1. via the idCAT web service of Consorci AOC, after which the subscriber must identify themself in person before one of the authorized Registration Authorities (city halls, regional government offices, etc.); or
2. by going to the offices of any Registration Authority that offers the service directly to fill out the application form and follow the instructions set out therein.

Through the Registration Authorities, EC-CIUTADANIA ensures that the applications are complete, accurate and duly authorized.

With regard to applications that are submitted in person by the Applicant at any of the Registration Authorities, once the registration agent has verified the identity of the applicant and the documents submitted by the latter to evidence their identity, the applicant and the agent shall sign the application and it will be sent to the EC-CIUTADANIA.

For applications that are filled out via the website before the Applicant identifies themself to the Registration Authority in person: If the agent notices some error in the data entered, when comparing them to the identification documents the applicant submits in person, the agent may make any changes necessary, provided that documentary record is kept

regarding the reason for the change; to which end the applicant will be asked to sign a data amendment document.

4.3.2. Legitimization to request a certificate

Before a certificate is issued and delivered, a certificate application must exist.

In the case of individual certificates, the applicant will be the subscriber themself, who in turn will be the private key holder.

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.

Note 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

El Registration Authority's agent shall validate the veracity and accuracy of the signatory's information and then inform the Certification Authority thereof.

The Registration Authority's agent shall validate the signatory's possession of the information to generate the signature (private key) that is 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. Certificate issuance

The Registration Authority's Agent shall produce the 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 agent of the Registration Authority. Once said validation takes place, the certificate shall be issued.

4.3.6. Notification of issuance to the subscriber

EC-CIUTADANIA shall notify the applicant indicating whether the certificate application submitted was approved or rejected.

If it is approved, EC-CIUTADANIA 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.

4.3.7. Delivery and protection of 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
    - Signature-creation and authentication device.
    - Software that is necessary to use the device.
    - Certificate-delivery slip.
- Simultaneously, the activation-key holder will be sent the certificate's activation information by email.

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

4.3.8. Certificate suspension

According to the provisions of the CPS.

4.3.9. Certificate revocation

According to the provisions of the CPS.

4.3.10. Certificate renewal

According to the provisions of the CPS.

5. Profile of the certificates issued under this Certification Policy

The following certificate types are issued under this Certification Policy:

Certificate type	**OID**
Qualified Citizenship Certificate (*idCAT certificat*)	1.3.6.1.4.1.15096.1.3.2.86.2

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