Consorci
Administració Oberta
de Catalunya

Certification Policy for
Public Sector Personal Certificates
Consorci AOC

Reference:	CP PERSONAL CERTIFICATES PUBLIC SECTOR
Version:	6.3
Date:	03/08/2020
OID:	1.3.6.1.4.1.15096.1.3.2.1.2

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/

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 Public Sector Personal 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
6.2	● Annual review of the documentation	31/03/2020
6.3	● Inclusion of qualified high-level and mid-level public worker authentication and signature certificates	03/08/2020

Contents

1. Introduction

1.1. Presentation and scope of application

The electronic Certificates referred to in this Certification Policy (CP) are issued by the Consorci AOC for use by public employees and workers of the 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 in 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 AOC Consortium 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, and persons associated.

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 EU Regulation 910/2014.

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

- Authentication high-level certificate for public employee (*T-CAT autenticació*).
- Qualified signature high-level certificate for public employee (*T-CAT signatura*).
- Qualified authentication and signature mid-level certificate for public employees (*T-CATP*).
- Authentication high-level certificate for public employees with pseudonyms (*T-CAT pseudònim autenticació*).
- Qualified signature high-level certificate for public employees with pseudonyms (*T-CAT pseudónim signatura*).
- Qualified authentication and signature high-level certificate for associated persons (*T-CAT persona vinculada*).
- Qualified authentication and signature mid-level certificate for associated persons (*T-CATP persona vinculada*).
- Qualified authentication and signature certificate for representatives acting before the Public Administrations (*T-CAT Representant*).
- Qualified authentication and signature high-level certificate for public worker (*T-CAT treballador públic*)
- Qualified authentication and signature mid-level certificate for public employees (*T-CATP treballador públic*)

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 Personal Certificates Public Sector
Version:	6.3
Description	Certification Policy for Public Sector Personal Certificates
Date of issue:	03/08/2020
OID:	1.3.6.1.4.1.15096.1.3.2.1.2
Location:	https://www.aoc.cat/catcert/regulacio/

1.2.2. Identification of certification policies for each certificate type

Type of certificate	**OID**
Authentication high-level certificate for public employee (*T-CAT autenticació*)	1.3.6.1.4.1.15096.1.3.2.7.1.2
Qualified signature high-level certificate for public employee (*T-CAT signatura*)	1. 3.6.1.4.1.15096.1.3.2.7.1.1
Qualified authentication and signature mid-level certificate for public employees (T-CATP)	1.3.6.1.4.1.15096.1.3.2.7.3.1
Authentication high-level certificate for public employees with pseudonyms (*T-CAT pseudònim autenticació*)	1.6.1.4.1.15096.1.3.2.4.1.23
Qualified signature high-level certificate for high-level public employees with pseudonyms (*T-CAT pseudónim signatura*)	1.3.6.1.4.1.15096.1.3.2.4.1.1
Qualified authentication and signature high-level certificate for high-level associated persons (*T-CAT persona vinculada*)	1.3.6.1.4.1.15096.1.3.2.82.1
Qualified authentication and signature mid-level certificate for associated persons (*T-CATP persona vinculada*)	1.3.6.1.4.1.15096.1.3.2.86.1
Qualified authentication and signature certificate for representatives acting before the Public Administrations (*T-CAT Representant*)	1.3.6.1.4.1.15096.1.3.2.8.1.1
Qualified authentication and signature high-level certificate for public worker (T-CAT treballador públic)	1.3.6.1.4.1.15096.1.3.2.82.2

Qualified authentication and signature mid-level certificate for public worker (T-CATP treballador públic)	1.3.6.1.4.1.15096.1.3.2.86.3

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

2.2. Registration authorities

Registration authorities are the individuals or companies that help 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-SECTORPUBLIC 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, hereinafter RA Operator).

There are two types of EC-SECTORPUBLIC registration authorities:

1. Subscriber entities, operated by a certificate subscriber entity
2. Registration authorities, which collaborate with EC-SECTORPUBLIC in 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 secure 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 signatories or key holders.
- The 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 TSP – 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 that are identified in the “Subject” field of the certificate.

2.3.3. Key holders or signatories

Key holders or signatories are individuals that have exclusive possession of the certified electronic signature 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. Said individuals must be duly identified in the certificate, indicating their first and last names, or via the use of a pseudonym.

The key holders or signatories are responsible for keeping the information necessary to generate the signature or authentication associated with the electronic certificate, under their custody.

2.3.4. Third party that relies on the certificates

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 n. 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 electronic certificates issued under this Certification Policy shall be valid for 5 (five) years from their issuance date, provided that the relevant certificate has not been suspended or revoked.

3.2. Signature-creation devices

The following certificates, issued pursuant to this Certification Policy, use a qualified signature-creation device in compliance with the requirements established under Annex II of EU Regulation 910/2014:

- Qualified authentication and signature certificates for high-level public employees (*T-CAT autenticació* and *T-CAT signatura*).
- Qualified authentication and signature certificates for high-level public employees with pseudonyms (*T-CAT pseudònim autenticació* and *T-CAT pseudónim signatura*).
- Qualified authentication and signature certificates for high-level associated persons (*T-CAT persona vinculada*).
- Qualified authentication and signature certificates for representatives acting before the Public Administrations (*T-CAT Representant*).
- Qualified authentication and signature high-level certificate for public worker (T-CAT treballador públic).

The rest of the certificates issued under this Certification Policy are issued in software.

3.3. 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.

3.3.1. 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:

Type of Certificate	**Scope of application**
Authentication high-level certificate for public employees (*T-CAT **autenticació***)	● Authentication of individual and attributes
Qualified signature high-level certificate for public employees (*T-CAT signatura*)	● Electronic signature

Qualified authentication and signature mid-level certificate for public employees (T-CATP)	● Authentication of individual and attributes ● Electronic signature
Authentication high-level certificate for public employees with pseudonyms (*T-CAT **pseudònim autenticació***)	● Authentication of individual and attributes
Qualified signature high-level certificate for public employees with pseudonyms (*T-CAT pseudónim signatura*)	● Electronic signature
Qualified authentication and signature high-level certificate for associated persons (*T-CAT persona vinculada*)	● Authentication of individual and attributes ● Electronic signature
Qualified authentication and signature mid-level certificate for associated persons (*T-CATP persona vinculada*)	● Authentication of individual and attributes ● Electronic signature
Qualified authentication and signature certificate for representatives acting before the Public Administrations (*T-CAT Representant*)	● Authentication of individual and attributes ● Electronic signature
Qualified authentication and signature high-level certificate for public worker (T-CAT treballador públic)	● Authentication of individual and attributes ● Electronic signature
Qualified authentication and signature mid-level certificate for public worker (T-CAT treballador públic)	● Authentication of individual and attributes ● 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.

3.3.2. 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

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

Website of the 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

The filling out the application is the first step the subscriber must take to get the certificates for its staff.

In the case of the Public Administrations and the entities that make up the public sector in accordance with article 3 of Law 29/2010, of August 3, on the use of electronic media in the public sector of Catalonia, the request will be sent

- Through the T-CAT registration authorities
- Directly to Consorci AOC, if the entity does not have a Registration Authority assigned to it. In such cases, Consorci AOC will act as the T-CAT Registration Authority.

The application requires that a document be sent containing the specific and certified information regarding the persons, entities or devices for which the certificate is being sought. The application must be signed by the person that is authorized for such purpose at the subscribing entity and the certification of such information must be attached thereto.

A physical address may also be confirmed, along with any other information that would allow the future key holder to be contacted directly.

All documents shall be delivered electronically to the Registration Authority. Documents may also be delivered in hard copy or via email, under exceptional circumstances, such as those set out below:

- That the entity subscriber, due to their legal nature, cannot be a user of the computer application that is used to send the applications (currently EACAT).
- That the subscriber is an entity that is requesting electronic certificates for the first time; meaning it does not have any electronic certificate to carry out the application process electronically.

4.3.2. Legitimization to apply for a certificate

A certificate application must be submitted before a certificate can be issued and delivered.

In the case of individual certificates, the applicant will be the subscriber him/herself. The subscriber will also be the holder of the private keys.

There must be an electronic or a hard-copy document signed by the Registration Authority, said document shall indicate the person or persons to be authorized by the relevant Certification Authority, to make requests.

The final user information that is necessary to submit the application will be entered by the applicant.

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 of this policy or of 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, particularly if they are exchanged with the subscriber (individuals certificates) or with a third-party applicant, as the case may be.
- 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

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

The RA 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 RA 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. Delivery and protection of activation information

To provide activation information with the maximum protection possible, Consorci AOC undertakes to distribute the elements of the certificates 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
    - Cryptographic device or software with the certificates
    - 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.

4.3.7. Suspension of certificates

According to the provisions of the CPS.

4.3.8. Revocation of certificates

According to the provisions of the CPS.

4.3.9. Renewal of certificates

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:

Type of Certificate	**OID**
Authentication certificate for high-level public employee (*T-CAT autenticació*)	1.3.6.1.4.1.15096.1.3.2.7.1.2
Qualified signature certificate for high-level public employee (*T-CAT signatura*)	1.3.6.1.4.1.15096.1.3.2.7.1.1
Qualified authentication and signature certificate for mid-level public employees (T-CATP)	1.3.6.1.4.1.15096.1.3.2.7.3.1
Authentication certificate for high-level public employees with pseudonyms (*T-CAT pseudònim autenticació*)	1.3.6.1.4.1.15096.1.3.2.4.1.2
Qualified signature certificate for high-level public employees with pseudonyms (*T-CAT pseudónim signatura*)	1.3.6.1.4.1.15096.1.3.2.4.1.1
Qualified authentication and signature certificate for high-level associated persons (*T-CAT persona vinculada*)	1.3.6.1.4.1.15096.1.3.2.82.1
Qualified authentication and signature certificate for mid-level associated persons (*T-CATP persona vinculada*)	1.3.6.1.4.1.15096.1.3.2.86.1
Qualified authentication and signature certificate for representatives acting before the Public Administrations (*T-CAT Representant*)	1.3.6.1.4.1.15096.1.3.2.8.1.1
Qualified authentication and signature high-level certificate for public worker (T-CAT treballador públic)	1.3.6.1.4.1.15096.1.3.2.82.2
Qualified authentication and signature mid-level certificate for public worker (T-CATP treballador públic)	1.3.6.1.4.1.15096.1.3.2.86.3

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