Consorci AOC PKI Disclosure Statement (PDS) for electronic certificates

Reference: PDS-CAOC-180509_v1.1_EN

Version: 1.1

Date: 09/05/2018

PAST VERSIONS

Version	Date	Section and Changes
1.0	21/02/2017	Initial Version
1.1	09/05/2018	Format corrections Added “Website authentication and SSL certificates issues” section Modified URL for CPS

INDEX

1. INTRODUCTION AND CONTACT INFORMATION

1.1. Introduction

This document is an informative text that aims to highlight the basics contained in the Certification Practice Statement (hereinafter CPS) and Certification Policy (hereinafter CP) of Catalonia's Open Administration Consortium (hereinafter Consorci AOC) with regard to electronic certificates. By no means is this document intended to develop, expand or amend the aforementioned CPS, CP from Consorci AOC.

This informative text is subject to the documentary hierarchy derived from the seventh clause herein, which must be respected and will be applicable at all times.

1.2. Responsible organisation

Catalonia's Open Administration Consortium (Consorci AOC)

Carrer Tanger, 98

08008 - Barcelona

1.3. Organisation's contact details

For any questions, please contact:

Catalonia's Open Administration Consortium (Consorci AOC)

Subdirecció de Tecnologia i Serveis

Carrer Tanger, 98

08008 - Barcelona

1.4. Contact and revocation procedure

For any questions, please contact:

Catalonia's Open Administration Consortium (Consorci AOC)

Servei de Certificació Digital

Carrer Tanger, 98

08008 - Barcelona

1.5. Website authentication and SSL certificates issues notification

To notify any any concern related with the usage, correctness, security or other regarding any kind of website authentication or SSL certificate issued by the Responsible Organization, please contact to the Organization's contact details of 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

2. TYPES AND PURPOSE OF CERTIFICATES

2.1. Definitions about recipients

- **Public employee:** catalan public administration's staff or when participation of civil Catalan administration exceeds 50%.
- **Related person:** Catalan's public administration's external staff, who need this certificate for dealings with public administration.
- **Public employee with pseudonym:** Catalan public administration's staff where person identification takes place through a pseudonym for special cases in which the certificate must conceal the identity of the public employee.
- **Representative:** the holder is an employee of the Catalan public administrations who acts as a representative of his/her agency with regard to other public authorities.
- **Legal person:** it refers to the identification of one catalan's public administration entity

2.2. Definitions on the use of certificates

- **Authentication**: identification of the person to allow access to a computer application.
- **Encryption:** use for encryption and decryption of files, to allow confidential handling.
- **Advanced electronic signing**: electronic signature carried out with a qualified certificate, pursuant to applicable legislation.
- **Qualified electronic signature:** qualified electronic signature carried out with a

qualified certificate that works with a secure device for creating an electronic signature.

- **Web security:** for client web applications identification, and to protect the privacy of client - server communication. The following variants may be obtained t:
    - **Online security for official sites**: intended to provide secure communications with the official sites of public Catalan agencies.
    - **Extended Validation**: ensure automatic browser validation.
- **Automated identification and signature**: when the identification and electronic signature is required for an application, rather than a person. The following variant can be obtained:
    - **Automated administrative action**: used for identification and authentication in automated administrative proceedings (electronic automated file, electronic copies and certifications, etc.).

2.3. Type of certificates

Type of certificates	Recipients	Purposes	OID	Validity
T-CAT Authentication	Public employee	Authentication	1.3.6.1.4.1.15096.1.3.2.7.1.2	Up to 5 years
T-CAT Signature	Public employee	Qualified signature	1.3.6.1.4.1.15096.1.3.2.7.1.1	Up to 5 years
T-CAT Related Person	Related person	Authentication Qualified signature	1.3.6.1.4.1.15096.1.3.2.82.1	Up to 5 years
T-CAT P	Public employee	Advanced authentication signature	1.3.6.1.4.1.15096.1.3.2.7.3.1	Up to 5 years
T-CAT P Related Person	Related person	Advanced authentication signature	1.3.6.1.4.1.15096.1.3.2.86.1	Up to 5 years
T-CAT Pseudonym Authentication	Public employee using pseudonym	Authentication	1.3.6.1.4.1.15096.1.3.2.4.1.2	Up to 5 years
T-CAT Pseudonym Signature	Anonymous related person	Qualified signature	1.3.6.1.4.1.15096.1.3.2.4.1.1	Up to 5 years

T-CAT R	Representative to public administrations	Authentication Qualified signature	1.3.6.1.4.1.15096.1.3.2.8.1.1	Up to 5 years
SSL device	Public employee	Site security	1.3.6.1.4.1.15096.1.3.2.51.1	Up to 3 years
Medium-level e-office	Legal person	Security for official Catalan public administration sites	1.3.6.1.4.1.15096.1.3.2.5.2	Up to 2 years
SSL EV device	Legal person	Extended validation	1.3.6.1.4.1.15096.1.3.2.51.2	Up to 2 years
Application device	Legal person	Automated identification and signature	1.3.6.1.4.1.15096.1.3.2.91.1	Up to 5 years
Medium-level seal	Legal person	Administrative actions	1.3.6.1.4.1.15096.1.3.2.6.2	Up to 5 years
idCAT Certificate	Citizens	Advanced authentication signature	1.3.6.1.4.1.15096.1.3.2.86.2	Up to 5 years

2.4. Certificate Validation

CRLs are posted on the website of Consorci AOC and the URLs identified in the issued certificates.

2.5. Issuing Certification Agency

The certificates are issued by a Certification Agency belonging to the public certification hierarchy in Catalonia.

3. USAGE LIMITS

Certificates will be used in accordance with their own function and purpose, and they may not be used for other functions and other purposes. Likewise, certificates must be used only in accordance with applicable law, especially given existing import and export restrictions at any given moment.

The Key Usage extension will be used to set technical usage limits for a private key corresponding to a public key listed in a X.509v3 certificate. It should be noted that the

effectiveness of restrictions based on certificate extensions sometimes depends on the operation of computer applications that have not been developed or cannot be controlled by Consorci AOC.

Certificates are not designed, and their use or resale is not authorised, as control equipment for hazardous applications or for uses requiring fail-safe measures, such as operation in nuclear facilities, navigation systems, air communications or weapon systems, where a mistake could lead directly to death, personal injury or serious environmental damage.

3.1. Usage limits aimed at subscribers

Subscribers must use the digital certification service provided by Consorci AOC exclusively for purposes authorised by the “Specific service terms” stated concisely in the fourth clause of this informative text.

Likewise, subscribers undertake to use the digital certification service in accordance with the instructions, manuals and procedures provided by Consorci AOC.

Subscribers must comply with any laws and regulations that may affect their right to use the cryptographic tools in question.

Subscriber cannot subject Consorci AOC digital certification services to inspection, alteration or reverse engineering measures without express written permission from Consorci AOC.

3.2. Usage warnings aimed at verifiers

Certificate verifiers must use the information service provided by Consorci AOC exclusively for authorised purposes, which are concisely listed in the fifth clause herein.

Likewise, verifiers undertake to use the information service in accordance with the instructions, manuals and procedures supplied by Consorci AOC.

Verifiers should comply with any law and regulation that may affect their right to use the cryptographic tools in question.

Verifiers cannot subject Consorci AOC digital certification services to inspection, alteration or reverse engineering measures without express permission in writing from Consorci AOC.

3.3. Evidence log

Records related to the lifecycle of certificates will be stored, either on paper or electronically, ensuring the appropriate security, authenticity, integrity, preservation and conservation methods related to the information contained in the certificate, for a period of 15 years. These records must be available to the Associated Certification Body.

Likewise, the certificate delivery sheets will be saved for a period of 15 years. These records must be available to the Associated Certification Body.

4. SUBSCRIBER OBLIGATIONS

4.1. Certificate request and key generation

Prior to the issuance and delivery of a certificate, there must be a certificate request.

Such request for issuing a certificate implies the subscriber's authorisation of Consorci AOC for it to generate its keys, and for it to issue the corresponding certificate. The key format and intended use will vary according to the profile.

The subscriber agrees to request the certificate based on:

- the specifications provided for each certificate
- the procedure stipulated in the CPS and the documentation of operations of the Consorci AOC, in addition to
- the technical components supplied by the latter, if necessary.

4.2. Accuracy of information

The subscriber assumes responsibility for all the information included, by any means, in the certificate application and that the certificate is accurate and complete for the corresponding purpose, and up-to-date at all times.

The subscriber has to report immediately to the Consorci AOC any inaccuracies detected in Consorci AOC's certificate once issued, as well as changes in the information provided and/or recorded for issuing the certificate.

In the event that the keys holder ceases its relationship with the subscriber, the latter must immediately request the revocation of the certificate.

4.3. Delivery and acceptance of the service

By signing the delivery slip, the subscriber, and where applicable, the key holder, acknowledges delivery of the certificate, the private key and any other technical format delivered by the Consorci AOC and, when applicable, the personal identification code. The subscriber will likewise confirm that these elements are working properly.

The subscriber, and where applicable the key holder accepts — by signing the delivery slip or via the electronic certificate acceptance procedure — the certificate as specified in the General Certification Policy of the Consorci AOC.

The subscriber must manage the signature of the key holder delivery slip and

safeguard it for a period of fifteen (15) years. All the information will be available to Consorci AOC, except when the certificate activation occurs by electronic means.

4.4. Key holder

The subscriber agrees to inform those responsible for key safeguarding of the terms and conditions governing the use of certificates.

Likewise, the subscriber agrees that the key holders fulfil their obligations as stipulated in the corresponding delivery slip.

4.5. Safeguarding obligations

The subscriber undertakes to, where necessary, safeguard the personal identification code, the card or any other technical format delivered by Consorci AOC, the private keys and, if necessary, the specifications owned by Consorci AOC that may have been supplied.

In the event of loss or theft of the private key for the certificate, or if the subscriber suspects that the reliability of the private key has been undermined for any reason, he/she must immediately notify Consorci AOC.

4.6. Proper use obligations

The subscriber must use the digital certification service, the public and private keys, the card or any other technical format delivered by Consorci AOC solely for purposes authorized in the General Certification Policy in accordance with the “Specific service terms” as well as any other instruction, manual and procedure supplied to subscribers by Consorci AOC. The subscriber will recognise that when using the certificate, and while it has not expired or has been suspended or revoked, accepts the certificate and it will be operational.

4.7. Prohibited transactions

Subscribers agree not to use their private keys, certificates, cards or any other technical format delivered by Consorci AOC in carrying out transactions prohibited by applicable law.

Consorci AOC’s digital certification services are not designed nor do permit use or resale as control equipment in hazardous situations, or for uses requiring fail-safe measures, such as operation in nuclear facilities, air navigation or communication systems, air traffic control systems or weapons control, where an error could directly cause death, bodily injury or serious environmental damage.

The certificates are issued to subscribers for the uses expressly listed in the first

section of the second clause of this informative text.

Any other use diferent from those described in this clause is expressly excluded and formally prohibited.

5. VERIFIER OBLIGATIONS

5.1. Informed consent

Consorci AOC informs verifiers that they have access to enough information to make an informed decision when verifying a certificate, and they can rely on the information contained therein.

Verifiers acknowledge that the use of Consorci AOC's Register and Certificate Revocation Lists (hereinafter "the CRLs") is governed by Consorci AOC's General Certification Policy and undertakes to comply with the technical, operational and security requirements detailed in the aforementioned Policy.

5.2. Electronic signature verification requirements

In order to rely on an electronic signature, it is essential for verifiers to check the existence and validity of both the certificate and the electronic signature, by implementing the verification procedure.

Verification involves checking the authenticity and integrity of the electronic document signed, in order to determine that it was indeed generated by the legitimate certification agency, i.e. the Consorci AOC, using the private key corresponding to the public key contained in the subscriber's certificate and that the document was not modified since the electronic signature was generated.

Certificate authentication will be performed automatically by the verifier's software based on services and, in any case, in accordance with the General Certification Policy and the following requirements:

- Using appropriate software to verify the certificate digital signature, authorised key algorithms and length and/or carry out any other cryptographic operation and establish the certificates chain on which the electronic signature being checked is based, since the electronic signature is verified using this certificate chain.
- Ensuring that the certificate chain identified is the most appropriate for the electronic signature being verified, since an electronic signature can be based on more than one certificate chain, and it is up to the verifier to ensure that the most appropriate chain is used for verifying.
- Checking the revocation status of certificates in the chain with the information provided in the Consorci AOC Register (with CRLs for instance) to determine

the validity of all certificates in the certificate chain, given that an electronic signature can only be deemed to be properly verified if each and every one of the certificates in the chain are correct and in force.

- Ensure that all certificates in the chain authorise use of the private key certificate by the certificate subscriber and the key holder, due to the possibility that some licenses may include usage limits that prevent relying on the electronic signature being verified. Each certificate in the chain has an indicator that refers to applicable usage terms to be reviewed by verifiers.
- Technically verify the signature of all certificates in the chain before trusting the certificate used by the signatory.
- Determine the date and time when the electronic signature was generated, since the electronic signature can only be deemed properly verified if it was created within the validity period of the certificate chain on which it is based.
- Define the data that has been digitally signed, since these will be used in signature verification.
- Technically verify the signature itself with the signer's certificate endorsed by the certificate chain.

5.3. Due diligence

Verifiers have to act with the utmost diligence before relying on any Certificates. In particular, Verifiers undertake to use the electronic signature verification software with the appropriate technical, operational and security aptitude to properly execute the signature verification process, and shall be exclusively responsible for any damage that may result from the incorrect selection of such software.

The previous limitation shall not apply when Consorci AOC has provided the verification software to the Verifier.

The Verifier can trust a certificate if the following conditions concur:

- The electronic signature must be able to be verified pursuant to the requirements of section two of the fifth clause.
- The Verifier must have used updated revocation information when carrying out signature verification.
- The type and class of certificate has to be appropriate for the intended use.
- The Verifier shall take into account other additional limitations for use of the certificate as noted in any way in the certificate, including those not processed automatically by the verification software, included as reference in the certificate and contained in these usage terms. Specifically, a certificate does not grant rights and powers from Consorci AOC to the subscriber or key holder beyond the description of the certificate according to the second clause of this

informative text or other express indication of the Consorci AOC or the subscriber itself.

- Finally, trust has to be reasonable under the circumstances. If circumstances require additional guarantees, the Verifier must obtain these guarantees to substantiate reasonable trust.

In any case, the final decision in terms of trusting a verified certificate or not is exclusively up to the Verifier, who has to take an active attitude and who is required to access all the information prepared by Consorci AOC to take his or her decisions in a fully informed manner. In case of doubt, the Verifier should not trust the certificate.

5.4. Trust in an unverified signature

It is forbidden to trust or otherwise use a signed, unverified certificate.

If the Verifier trusts a certificate, he or she will assume all the risks of this action.

5.5. Verification effect

Based on the proper verification of a signature and/or certificate, in accordance with the usage terms, the Verifier can trust the certificate data and/or signature based on the former, within the corresponding usage constraints.

5.6. Correct use and prohibited activities

The Verifier undertakes not to use any certificate status information or any other information supplied by Consorci AOC in performing any act prohibited by the law applicable.

The Verifier undertakes not to inspect, interfere or reverse engineer the technical implementation of Consorci AOC public certification services without prior written consent of Consorci AOC.

Moreover, the Verifier undertakes to not intentionally compromise the security of Consorci AOC's public certification services.

Consorci AOC's digital certification services are not designed nor do they permit use or resale as control equipment in hazardous situations or for uses requiring fail-safe measures, such as operation in nuclear facilities, air navigation or communication systems, air traffic control systems or weapons control, where an error could cause death, bodily injury or serious environmental damage.

6. LIMITED WARRANTY AND DISCLAIMERS

6.1. Consorci AOC warranty for digital certification services

Consorci AOC undertakes to provide digital certification services in certain technical and operational conditions, as set out in its General Certificate Policy, including a Certificate Register, where the information regarding certificate status is published.

Consorci AOC undertakes to issue status information, including the suspension and revocation of certificates issued in accordance with the General Certification Policy.

Consorci AOC guarantees the following information service conditions:

- The certificate contains accurate and current information at the time of issuance, duly verified in accordance with the provisions of current legislation.
- The certificate meets all the requirements regarding content and format stipulated by the General Certification Policy.
- Consorci AOC private key has not been compromised, unless otherwise notified by the Register.

6.2. Disclaimer

Consorci AOC does not guarantee any software whatsoever used by anyone to create, verify or use in any way, any digital signature or digital certificate issued by Consorci AOC itself, except when there is a written declaration to the contrary.

6.3. Insurance

Consorci AOC, as a certification service provider, has guarantee enough to cover its liability under the law, unless it is exempted by law from this obligation.

In case of misuse or unauthorised use of certificates, Consorci AOC (or the relevant Associated Certification Body) does not act as a fiduciary agent for subscribers and third parties, who must directly address the person in breach of the usage terms set out by Consorci AOC (or Associated Certification Body involved).

7. APPLICABLE AGREEMENTS, CPS and CP

7.1. Applicable agreements

The agreements which apply to the certificate are listed in the “service-specific terms”.

7.2. Certification Practice Statement (CPS)

Consorci AOC certification services are technically and operationally regulated by the Certification Practice Statement, its subsequent updates, and additional documents.

The CPS can be found at:

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

Anything not covered in this informative text will be governed by the provisions of the Certification Practice Statement. Likewise, in case of contradiction between the terms of this informative text and the Certification Practice Statement of Consorci AOC, the latter shall prevail in any case.

7.3. Certification Policy (CP)

Consorci AOC has a certification policy detailing technical, legal, operational and regulatory requirements, as well as the regulation of certificates, available to the user community that requests them.

Any divergence arising from this informative text and the Certification Policy of the Consorci AOC will be resolved in favour of the latter.

Anything not covered in this informative text will be governed by the provisions of Consorci AOC's Certification Policy. Likewise, in case of contradiction between the terms of this informative text and the Consorci AOC's Certification Policy, the duly published Certification Policy shall prevail in any case.

8. PRIVACY POLICY

Consorci AOC cannot disclose or be compelled to disclose any confidential information concerning certificates without an advance specific request from:

a) the person with whom Consorci AOC is obliged to keep confidential information, or

b) a court, administrative order or any other order provided regarding current legislation.

However, the subscriber agrees that certain information, which might be personal or other kinds, provided in the certificate request will be included in certificates, and that the mechanism to check certificate's status, and that this information is not confidential, as stipulated by law.

Consorci AOC is not liable for any use made by a third party of this personal information.

9. REFUND POLICY

Not applicable.

10. LAW AND JURISDICTION

Parties shall be governed by Spanish law, particularly Law 59/2003, dated 19 December, on electronic signatures, and Regulation (EU) No. 910/2014 of the European Parliament and Council dated 23 July 2014 concerning electronic identification and trust services for electronic transactions in the internal market, repealing Directive 1999/93/EC (hereinafter eIDAS).

Jurisdiction is stipulated in Law 29/1998 dated 13 July, governing the Administrative Jurisdiction.

11. ACCREDITATIONS AND QUALITY SEALS

The Consorci AOC has passed the following audits:

- WebTrust for Certification Authorities.
- eIDAS Compliance.