Consorci
Administració Oberta
de Catalunya

Certification Practices Statement
Consorci AOC Certification Authority

Reference:	D1111_E0650_N-DPC Consorci AOC
Version:	6.8
Date:	29/03/2023

The original in force version of this document can be viewed in electronic format at Consorci AOC website and can be accessed via the following URL: https://www.aoc.cat/catcert/regulacio

Version history

Version	Summary of changes	Date
5.0	Adaptation to EIDAS	9/5/2018
6.0	Creation of a new unified certification practices statement. It is numbered version 6.0 for the purpose of document management.	26/07/2018
6.1	● Annual review of the documentation, post audit eIDAS. ● Aligned document with RFC 3647. ● "*1.1. Presentation*": indicated prevalence of the CA / Browser Forum guidelines on the CPD itself. ● "*1.5.5. Review frequency*": created section. ● "*4.4.3. Publication of the certificate*": indicated possibility of publication of certificates if express consent is available. ● "*4.10.7. Frequency of the Certificate Revocation List (CRL) publication*": added frequency of publication of the CRL. ● "*5.2.2. Number of persons per task*": specified the redundancy of roles for certain tasks. ● "*6.5.3. Frequency of revision of the configurations of trustworthy systems*": created section. ● "*9.4. Personal data protection*": tight descriptions and updated applicable legislation, including GDPR and the LOPDGDD. ● "*9.12.1. Modification procedures*": reformulated section ● Removed references to code signing. ● Congruence adjustments to the texts.	24/07/2019
6.2	● Adaptation to CAB-Forum requirements: aligned with all sections of RFC 3647 ● Inclusion of 1.6 "Definitions and Acronyms" ● Inclusion of 7.3: "OCSP Profiles"	31/03/2020
6.3	● Introduction of identification by videoconference in section 3.2.3 ● Other minor changes	21/05/2020
6.4	● Inclusion of authentication and signature certificates of public worker of mid and high level. ● Procedure for generating the last CRL in the event of a key compromise or termination of the service. Section 4.10.9	03/08/2020
6.5	● Adaptation to Law 6/2020, of November 11, regulating certain aspects of electronic trust services	27/01/2021
6.6	● Section 3.2.5: Verified information is added for SSL certificates	20/07/2021

	• Section 4.10.1: new revocation causes • Section 4.10.12: adaptation of the requirements for password compromise • Section 5.3.1: qualification of the validation specialist • Section 5.7.3: private key compromise adaptation • Section 6.1.9: adaptation of password usage purposes • Section 6.2.1.1: secure signature creation device qualification loss. • Section 7.1: certificate profile. Clarification of minimum entropy of the serial number. • Section 9.5.2: Intellectual property of the DPC and PCs. • Section 9.14: all applicable regulations are listed	
6.7	• Section 4.7.1: numeration modified from 4.8 to 4.7.1 according to the RFC3647 • Section 4.9.7: periodicity and CRL's emission time • Section 4.10.1: request about revocation status of expired certificates • Section 9.4.4: modified maximum notification period to the APDCAT • Section 9.6.4.1: additional verification instructions • Section 9.14: Update of the regulatory and security framework	08/06/2022
6.8	• Section 1.5.2 : update of organization contact information.	29/03/2023

Index

1. Introduction

1.1. Presentation

This document is the Certification Practices Statement (CPS) of Consorci Administració Oberta de Catalunya (Consorci AOC), the Catalonia public trust service provider (TSP) that operates according to Regulations (EU) nº 910/2014, related to electronic identification and trusted services for electronic transactions within the interior market and repealing the Directive 1999/93/CE (Regulation (EU) nº 910/2014).

This CPS details the group of practices adopted by Consorci AOC as Trust Service Provider for digital certificates issuance and trusted services based on the following standards: :

- ETSI EN 319 401 (General Policy Requirements for Trust Service Providers).
- ETSI EN 319 411-1 (Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements)
- ETSI EN 319 411-2 (Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates)
- ETSI EN 319 412-1 (Certificate Profiles; Part 1: Overview and common data structures)
- ETSI EN 319 412-2 (Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons)
- ETSI EN 319 412-3 (Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons)
- ETSI EN 319 412-4 (Certificate Profiles; Part 4: Certificate profile for web site certificates)
- ETSI EN 319 422 (Certificate profiles for time-stamping protocol and time-stamp token profiles)
- ETSI EN 319 412-5 (Certificate Profiles; Part 5: QCStatements)

The structure of this document is based on the “RFC3647 - Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework“ standard specification, created by the work group PKIX of IETF.

The current CPS correlates with the different Certification Policies (CP) developed for each typology of digital certificate issued under the control of Consorci AOC, which are described

in section 1.1.1 of the current document. In case of contradiction between the current CPS and certain CP, the provisions made within this document shall prevail.

The Digital Certification Service of Consorci AOC complies with the current version of Ca/Browser Forum standard for the issuance and management of extended validation certificates, and with the Baseline Requirements standards of this same organisation for the issuance of server device certificates (in catalan “certificats de dispositiu de servidor” or CDS), published at http://www.cabforum.org. The indications of the CA / Browser Forum guides will prevail over the CPS.

1.1.1. Certification types and classes

Consorci AOC provides its certification services with the purpose of issuing digital certificates for various applications and end users. All certificates issued by Consorci AOC comply with the requirements of Regulation (EU) nº 910/2014.

1.1.1.1. Citizen certificates

- **Qualified citizen certificate (idCAT):** idCAT certificate is a qualified certificate of identification and electronic advanced signature intended for citizens with catalan administrative neighborhood, and for others (collectively referred to as “subscribers”) who need to work with Public Administrations and other institutions of Catalonia.

1.1.1.2. Public Sector Personal Certificates

- **High-level authentication certificate for public servant (T-CAT autenticació).** Allows the identification of a public servant for the execution of their tasks, as a tool for being able to perform within the electronic environment of a Public Administration, body, public organisation or catalan public law entity according to applicable regulation. T-CAT Authentication certificates and T-CAT signature are issued and stored together in a unique cryptographic device.

- **High-level qualified certificate of signature for public servant (T-CAT signatura).** Allows the electronic signature of a public servant for the execution of their tasks, as a tool for being able to perform within the electronic environment of a Public Administration, body, public organisation or catalan public law entity according to applicable regulation. T-CAT Authentication certificates and T-CAT signature are issued and stored together in a unique cryptographic device.

- **Mid-level/Substantial-level qualified certificate of authentication and signature for public servant (T-CATP).** These certificates of authentication and signature are issued to catalan public servants in software format for the execution of their tasks for actions that do not require high-level security, according to applicable regulation.

- **High-level authentication certificate for public servant with pseudonym (T-CAT pseudònim autenticació).** These certificates shall be issued under the previous evaluation of pseudonym legal accreditation that must be contained within the

request. They will be specifically accepted for justified uses where the holder data can not be revealed, and by people who already have a regulated pseudonym within their organisation, such as prison workers, Mossos d'esquadra, social services, etc. The features of this certificate are the same as for T-CAT Authentication certificate, apart from those that relate to the pseudonym use. T-CAT with Pseudonym Authentication certificates and T-CAT with Pseudonym Signature certificates are issued and stored together in a unique cryptographic device.

- **High-level qualified certificate of signature for public servant with pseudonym (T-CAT pseudònim signatura).** For the issuance of these certificates the same circumstances as T-CAT with Pseudonym Authentication certificates shall be considered. The features of this certificate are the same as for T-CAT Signature certificate, apart from those that relate to the pseudonym use. T-CAT with Pseudonym Authentication certificates and T-CAT with Pseudonym Signature certificates are issued and stored together in a unique cryptographic device.

- **High-level qualified certificate for affiliate person of authentication and signature (T-CAT persona vinculada):** Personal identification and qualified electronic signature certificate with the option to state position. These certificates are issued and stored in software.

- **Mid-level/Substantial-level qualified certificate for affiliate person of authentication and signature (T-CATP Persona vinculada):** Personal identification and qualified electronic signature certificate with the option to state position. These certificates are issued and stored in software format.

- **Qualified certificate of authentication and signature for representative towards the Public Administration (T-CAT Representant)**: Personal identification and qualified electronic signature certificate with the option to state position. These certificates are issued and stored in a cryptographic device. They are intended for individuals and contain information regarding the holder that allows them and their organisation to be identified. They are provided to public employees of the public sector of Catalonia for use as identifying elements in electronic communications, allowing the signature of electronic format documents that make processes and online consultations possible. These certificates allow the identification as a person who holds a particular position in their organisation.
- **High level qualified certificate of authentication and signature of public worker (T-CAT treballador públic)**. Personal certificate for identification and qualified electronic signature, issued and stored in a cryptographic device. These certificates are intended for those persons who maintain a labor or senior management relationship in an entity that integrates the public sector of Catalonia.

- **Mid-level/Substantial-level qualified certificate of authentication and signature of public worker (T-CATP treballador públic)**. This type of authentication and signature certificates are issued for use in software by **public workers** in the Catalan

public sector in the exercise of their functions in actions that do not require a high level of security, in accordance with the provisions of the applicable regulations.

1.1.1.3. Devices and Infrastructure Certificates

- **Application Certificate (Dispositiu aplicació):** This certificate is stored in a server (preferably in a cryptographic device) and is required by an application in order to seal documents, files or messages for the purpose of assure its authenticity and integrity. Juridically it operates as an advanced electronic seal of the body or department of the Public Administration on which behalf it is issued, according to Regulation EU 910/2014, although its use remains limited to data exchange between applications.

- **Advanced Electronic Seal Certificate (Segell nivell mig/substancial)**: It is used for identification and authentication of documents, files or messages in the exercising of its functions for automatic administration for public services provision according to article 37 of Regulation UE 910/2014. This certificate can be used for data exchange (between administrations, administrations and citizens, and administrations and companies), identification and authentication of a system, web service or application, automatic electronic archive, attested copies and electronic copies, amongst others. These certificates are issued and stored in software format.

- **Electronic Office Certificate (Seu-e nivell mig/substancial)**: It is used to identify and guarantee the integrity and authenticity of the electronic office of a body, understanding the definition of electronic office as described in article 38 of Law 40/2015, of October 1st, on the legal regime of the public sector, and the settlement of secure communications.

  This certificate can be used for citizen secure connection to official websites, the authentication of a website, the hosting of electronic registers, the consultancy and authorisation of representation registers, etc..

  Since 2011, Consorci AOC issues the Electronic Office Certificate following the Standard Extended Validation SSL Certificate, which guarantees the maximum security level of the transactions made in the website.

- **Secure Socket Layer Certificate (Dispositiu SSL):** These certificates guarantee the identity of a domain towards the users who are connecting, confirming that the website is the original and valid, the domain is officially registered that it is not been replaced, and that no one has changed the published information or manipulated the registered data in the server in an unauthorised manner.

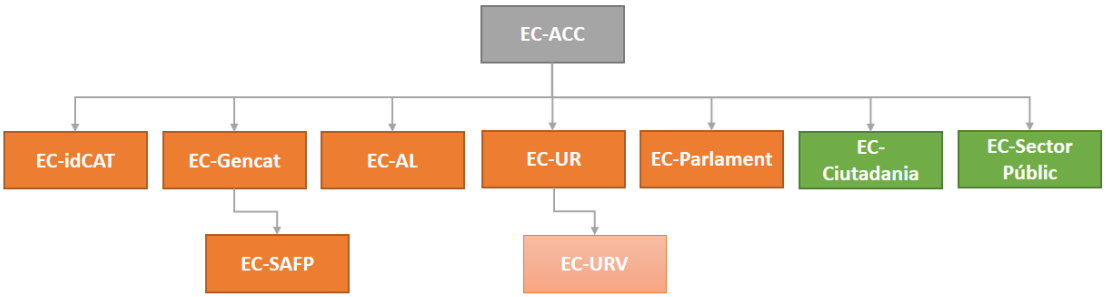
- **Secure Socket Layer Extended Validation Certificate (Dispositiu SSL EV):** SSL EV certificates are no different from SSL certificates regarding structure or function, but they have been issued by Certification Authorities that, like Consorci AOC, have achieved the strict security requirements established within the Standard Extended Validation SSL Certificate.

The main advantage of this is that new browsers will accept them immediately and they will show a security confirmation, that will allow users to quickly identify a secure and trusted site, since they are designed to show unique visual signals indicating EV certificate presence.

- **Qualified Time Stamp Certificate (Segell de temps):** These certificates guarantee the integrity of electronic files and communications at a particular date and time, using a reliable time source. Time Stamp Certificates issued by Consorci AOC comply with the established requirements of article 42 of Regulation (EU) nº 910/2014.

1.1.2. Hierarchies

As detailed in the following chart, Consorci AOC current certification hierarchy (since 2015) has been reduced to two Subordinate Certification Authorities (marked in green) and one Root Certification Authority:



EC-SectorPublic: sets issuance of certificates for Cataluña Public Sector, replacing the former Authorities EC-SAFP, EC-AL, EC-UR and EC-Parlamento. These Certification Authorities do not issue certificates anymore, although some certificates are still in force

Certificates issued under the former Certification Authorities EC-SAFP, EC-AL, EC-UR and EC-Parlamento are not regulated by this CPS version, but by CPS AL, GENCAT, SAFP, PARLAMENT, UR and URV in their versions 5.0, 2.0, 5.0, 2.0, 7.0, 4.0, corresponding to last update of each referred document before the cease of certificate issuance under the aforementioned Certification Authorities.

EC-Ciudadanía: issues digital certificates to citizens, replacing the former EC-idCAT which has also stopped issuing certificates, despite some certificates still being in force. Certificates issued under the former EC-idCAT Certification Authority are not regulated by this CPS version, but by CPS [idCAT] in its versión [4.0], corresponding to last update of the referred document before the cease of certificate issuance under the aforementioned Certification Authorities.

1.1.3. Test certificates issuance

Consorci AOC can issue test certificates signed by a real CA but with fictitious content for supervisor organisations, validation entities and application developers to be able to conduct their integration / evaluation processes for their purposes. Consorci AOC adds the following information to these certificates for all users to clearly identify that they are test certificates without responsibility:

Name of organisation	Test organisation

NIF of organización	VATES-Q0000000J
Address	Barcelona
Zip code	08008
Email address	scd@aoc.cat
First surname	de la Peça
Second surname	de Proves
DNI/NIE	00000000T

1.2. Document name and identification

1.2.1. Identification of this document

Name:	Certification Practices Statement (CPS)
Version:	6.8
Description	Consorci AOC Certification Practices Statement
Issuance date:	29/03/2023
OID:	1.3.6.1.4.1.15096.1.2.2
Location:	https://www.aoc.cat/catcert/regulacio

1.2.2. Identification of certification policies covered by this CPS

Type of certificate	OID	Policy
Citizen certificates		
Citizen certificate (idCAT)	1.3.6.1.4.1.15096.1.3.2.86.2	Citizen CP
Personal certificates for public sector		
High-level authentication certificate for public servant (T-CAT autenticació)	1.3.6.1.4.1.15096.1.3.2.7.1.2	Personal Certificates for Public Sector CP
High-level qualified certificate of signature for public servant (T-CAT signatura)	1. 3.6.1.4.1.15096.1.3.2.7.1.1	Personal Certificates for Public Sector CP
Mid-level/Substantial-level authentication and signature qualified certificate for public servant (T-CATP)	1.3.6.1.4.1.15096.1.3.2.7.3.1	Personal Certificates for Public Sector CP
High-level authentication certificate for public servant with pseudonym (T-CAT pseudònim autenticació)	1.3.6.1.4.1.15096.1.3.2.4.1.2	Personal Certificates for Public Sector CP
High-level authentication and signature qualified certificate for	1.3.6.1.4.1.15096.1.3.2.4.1.1	Personal Certificates for Public Sector CP

public servant with pseudonym (T-CAT pseudònim signatura)		
High-level authentication and signature qualified certificate for affiliated person (T-CAT persona vinculada)	1.3.6.1.4.1.15096.1.3.2.82.1	Personal Certificates for Public Sector CP
Mid-level/Substantial-level authentication and signature qualified certificate for affiliated person (T-CATP persona vinculada)	1.3.6.1.4.1.15096.1.3.2.86.1	Personal Certificates for Public Sector CP
Authentication and signature qualified certificate for representative towards Public Administration (T-CAT representant)	1.3.6.1.4.1.15096.1.3.2.8.1.1	Personal Certificates for Public Sector CP
High level qualified certificate of authentication and signature of public worker (T-CAT treballador públic)	1.3.6.1.4.1.15096.1.3.2.82.2	Personal Certificates for Public Sector CP
Mid-level/Substantial-level qualified certificate of authentication and signature of public worker (T-CATP treballador públic)	1.3.6.1.4.1.15096.1.3.2.86.3	Personal Certificates for Public Sector CP
Device and Infrastructure Certificates		
Application Certificate (Dispositiu aplicació)	1.3.6.1.4.1.15096.1.3.2.91.1	Device and Infrastructure CP
Advanced Electronic Seal Certificate (Segell nivell mig/substantial)	1.3.6.1.4.1.15096.1.3.2.6.2	Device and Infrastructure CP
Electronic Office Certificate (Seu-e nivell mig/substancial)	1.3.6.1.4.1.15096.1.3.2.5.2	Device and Infrastructure CP
Secure Socket Certificate (Dispositiu SSL)	1.3.6.1.4.1.15096.1.3.2.51.1	Devices and Infrastructures CP
Secure Socket Extended Validation Certificate (Dispositiu SSL EV)	1.3.6.1.4.1.15096.1.3.2.51.2	Device and Infrastructure CP
Qualified Time Stamp Certificate (segell de temps)	1.3.6.1.4.1.15096.1.3.2.111	Device and Infrastructure CP

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

1.3. Participating entities

1.3.1. Trusted services provider

According to the terminology contained within Regulation (UE) nº 910/2014 related to electronic identification and trusted services for electronic transactions within the interior market, Consorci AOC acts as Trusted Services Provider (TSP) in the context of this CPS, being responsible for the issuance and management of digital certificates generated in the certification hierarchy (PKI) referred previously in this document.

1.3.2. Root Certification Authority

Root Certification Authority is the entity in the referred certification hierarchy that issues certificates to other certification authorities and for which the public key has been auto signed. Its function is to sign the certificate for other Certification Authorities belonging to the referred certification hierarchy.

The Root Certificate identification details of Consorci AOC certification hierarchy are:

Root CA EC-ACC

CN:	EC-ACC
Hash:	88:49:7F:01:60:2F:31:54:24:6A:E2:8C:4D:5A:EF:10:F1:D8:7E:BB:76:62:6F:4A:E0:B7:F9:5B:A7:96:87:99
Validity:	07/01/2031
Type of Key:	RSA 2048

1.3.3. Subordinate Certification Authorities

We denominate Delegate or Subordinate Certification Authorities as those which issue end-entity certificates in the certification hierarchy, and whose public key certificates have been digitally signed by the Root Certification Authority.

Subordinate Certification Authorities identification details operated by Consorci AOC under this CPS are:

CA EC-CIUTADANIA

CN:	EC-Ciutadania
Hash:	0F:D9:9A:AE:1F:FC:D5:D9:F0:AD:76:ED:DD:CB:EF:6B:88:4C:C8:5C:16:BF:CF:A4:B5:24:61:55:D6:59:7E:D6
Validity:	18/9/2030
Type of key:	RSA 2048

CA EC-SECTORPUBLIC

CN:	EC-SectorPublic
Hash:	35:6A:5F:4D:99:4E:9E:FA:7C:AE:FC:49:17:68:91:1D:65:EC:25:97:74:65:B6:10:E2:F2:9A:A4:47:26:31:C3
Validity:	18/9/2030
Type of key:	RSA 2048

1.3.4. Register Authority

Register Authorities are the natural or legal persons who support Certification Authorities with specific procedures and relationships with certificate applicants and subscribers, particularly in identification processes, registration and authentication of certification subscribers and key holders.

1.3.5. End users

End users are those individuals who obtain and use electronic certificates. We can distinguish them as follows:

- Certificate requesters.
- Certificate subscribers.
- Signatories or key holders.
- Relying parties.

1.3.5.1. Certificate Applicants

An applicant is the individual who, on their own behalf or as representative of a relying party, requests the issuance of a digital certificate.

The prerequisite requirements that an applicant must have will depend on the type of the requested certificate, as described in the CP applicable to each type of certificate.

1.3.5.2. Certificate subscribers

A subscriber is the natural or legal person who contracts Consorci AOC delivery services.

In some cases the subscriber will be able to act as Point of Verification in Person, assuming part of the registration functions and taking responsibility towards Consorci AOC, its Register Authorities and End Users for:

- Correct identification of certificate applicants and signatories for which the subscriber is acting as Point of Verification in Person.
- Truthfulness and accuracy of the formally required submitted documentation for each type of certificate.
- Attested copy of original documents submission.
- Custody and delivery of referred documentation to Consorci AOC in case of being requested.
- Certificate delivery to signatories or key holders.

1.3.5.3. Key holders or signatories

A key holder or signatory is a natural person who exclusively possesses certificate electronic signature or authentication keys, either acting on their own behalf, in representation of an organisation or via other type of association.

These persons must be duly identified within the certificate through their name and surname or a pseudonym, likewise their organisation must be uniquely identified.

The signatory or key holder is responsible for the custody of the signature creation data associated with the electronic certificate.

1.3.5.4. Relying parties

A relying party is a person or organisation that voluntarily trusts in a certificate issued under certain Consorci AOC certification hierarchies

Consorci AOC obligations and responsibilities towards relying parties shall be limited to those described in this CPS, in the Regulation (UE) nº 910/2014 and in the general rules that result from application.

Relying parties that trust in these certificates should acknowledge their limitations of use.

1.4. Usage of Certificates

This section lists the applications for each type of certificate, establishing limitations and prohibiting certain certificates applications.

1.4.1. Typical usage of certificates

Consorci AOC certificates can be used within the terms of the corresponding CP.

1.4.2. Prohibited uses

Certificates may only be used within the usage limits specifically described in this CPS and the corresponding CP. Any other use not described in the referred documents is expressly excluded from the contractual scope and formally prohibited. Certificates must not be used for any illegal purpose.

Certificates have not been designed for, cannot be intended for, and are not authorised for use or resale within control equipment for dangerous situations or for uses that require error test actuations, like nuclear facility functioning, navigator systems or air communications, or gun control, where an error could involve immediate death, personal injury or severe environmental damage.

End user certificates cannot be used for signing any type of public key certificates or certificates revocation lists.

1.5. Practices Statement Management

1.5.1. Responsible Organisation for managing the specification

Consorci Administració Oberta de Catalunya – Consorci AOC

1.5.2. Organization contact information

Consorci Administració Oberta de Catalunya – Consorci AOC

Registered Office: Tànger, 98, planta baixa (22@ Edifici Interface) - 08018 Barcelona

Website of Consorci AOC: www.aoc.cat

Website of Consorci AOC digital certification service: 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.

1.5.3. Person who determines the conformity of a Certificate Practices Statement (CPS) with the policy

The person who determines the conformity of a CP with the CPS is the Consorci AOC Digital Certification Service Responsible, based on the results of an audit for this purpose, conducted biannually by a third party.

1.5.4. Approval procedures

Consorci AOC documentation and organisation system guarantees, through the application of corresponding procedures, the correct maintenance of the CPS and the service specifications publication procedure.

Initial version of this CPS is approved by the Consorci AOC Executive Commission, which is the Consorci AOC executive direction body. The Consorci AOC Managing Director is authorised to approve modifications in the CPS.

1.5.5. Review frequency

The CPS, the different CP and the PKI Disclosure Statements (PDS), will be reviewed and, if necessary, updated annually. The aforementioned documents will be reviewed and modified when there is any change that their content may be affected, such as legislative modifications, changes in infrastructure or changes in the services operation, among others.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

- Certification Services Provider: natural or legal person that issues electronic certificates or provides other services in relation to the electronic signature.
- Trust Services Provider (TSP): natural or legal person that provides one or more trust services, either as a qualified provider or as an unqualified provider of trust services.
- Electronic Certificate: a document electronically signed by a trusted service provider that links the signature verification data to a signer and confirms their identity.
- Qualified Certificate: Certificate issued by a TSP, which meets the requirements established in Annex I of Regulation (EU) nº 910/2014 (eIDAS) and in article 7 of Law 6/2020, of November 11, regarding the verification of the identity and other circumstances of the applicants, and the reliability and guarantees of the trust services they provide, in accordance with Title III of the aforementioned Law 6/2020, of November 11.
- Public Key and Private Key: the asymmetric cryptography on which the PKI is based uses a pair of keys in which what is encrypted with one of them can only be decrypted with the other and vice versa. One of these keys is called public and is included in the

electronic certificate, while the other is called private and is only known by the certificate holder.

- Conformity Assessment Body: bodies accredited by member states to be able to issue conformity reports as required by Regulation (EU) No. 910/2014.
- Signature Creation Data (Private Key): this is unique data, such as codes or private cryptographic keys, that the signer uses to create the electronic signature.
- Signature Verification Data (Public Key): is the data, such as public cryptographic codes or keys, that are used to verify the electronic signature.
- Qualified Electronic Signature / Stamp Creation Device (DCCF): Electronic signature creation device that meets the requirements listed in Annex II of Regulation (EU) nº 910/2014.
- Electronic Signature: data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign, can be used as a means of personal identification.
- Advanced Electronic Signature: electronic signature that allows establishing the personal identity of the signatory with respect to the signed data and verifying the integrity of the same, as it is exclusively linked to both the signatory and the data to which it refers, and for having been created by means that it maintains under its exclusive control.
- Qualified Electronic Signature: It is an advanced electronic signature which is based on a qualified certificate and generated by a secure / qualified signature creation device.
- Hash function: it is an operation performed on a data set of any size, so that the result obtained is another fixed-size data set, regardless of the original size, and which has the property of being uniquely associated with the initial data.
- Lists of Revoked Certificates (CRL or LCR): list of relationships of revoked or suspended certificates.
- Hardware Cryptographic Module (HSM): hardware module used to perform cryptographic functions and store keys in safe mode.
- Electronic Time Stamp: it is a special type of electronic signature issued by a trusted third party that guarantees the integrity of a document at a specific date and time.
- Qualified Electronic Time Stamp: it is an electronic time stamp that meets the requirements established in article 42 of Regulation (UE) nº 910/2014.
- Time Stamping Authority (TSA): Trusted entity that issues time stamps
- Validation Authority (VA): Trusted entity that provides information on the validity of digital certificates and electronic signatures.

1.6.2. Acronyms

AOC:	Open Administration of Catalonia
CA:	Certification Authority
CP:	Certificate Policy
DPC:	Certification Practices Statement
ETSI:	European Telecommunications Standard Institute
HSM:	Hardware Security Module
IETF:	Internet Engineering Task Force
LDAP:	Lightweight Directory Access Protocol
LRC:	Certificate Revocation List
OCSP:	Online Certificate Status Protocol
OID:	Object identifier
PDS:	PKI Disclosure Statement
PKI:	Public Key Infrastructure
PSC:	Trust Services Provider

2. Publication of certificate information and directory

2.1. Certificates directory

Certificates directory service is available on a 24x7 basis. In cases of error beyond the control of the Certification Authority, the Authority will work with reasonable efforts to get the service available as soon as possible within the period stipulated in section 5.7.4 of this CPS.

2.2. Information publication of the Certification Authority

The Certification Authority publishes the following information on its website (http://www.aoc.cat/catcert/regulacio):

- Revocated certificates lists and other certificate revocation status information.
- Certificate and revocation lists profiles.
- The CPS.
- The CP applicable to each type of certificate.
- The PKI Disclosure Statement (PDS).

Any changes to the specifications or service conditions is notified to the users by the Certification Authority through the directory.

In all cases there will be explicit references made to such changes within the homepage of the service website.

The previous version is maintained but it will be indicated that it has been replaced by a new version.

2.3. Frequency of publication

Certification Authority information is published as it becomes available, and in particular immediately when updates related to certificate validity are to be issued.

Changes to this document are regulated by the terms stipulated in section 9.12.1.

15 days after the publication of the new version, the reference on the homepage is removed and inserted into the directory.

Former versions of the documentation are kept during a period of 15 (fifteen) years by the Certification Authority. They may be consulted for those who are interested.

Certificates revocation status information is published according to section 4.10.7.

2.4. Access control

The CPS, CP, PDS (PKI Disclosure Statements), CA Certificates and CRL are published in public data repositories without access control.

3. Identification and authentication

3.1. Name management

This section outlines requirements used in identification and authentication procedures during the Register Authorities operations, prior to certificate issuance and delivery.

3.1.1. Types of names

3.1.1.1. Syntactic Structure

All certificates contain a unique X.501 name in the field Subject, including a CommonName (CN=) component.

Syntactic structure and each certificate field content, as well as its semantic significance, are described in the document “certificate profiles” that Consorci AOC publishes in its website (http://www.aoc.cat/catcert/regulacio).

3.1.1.2. Certificate profiles

Certificate profiles are published on Consorci AOC website (http://www.aoc.cat/catcert/regulacio).

3.1.2. Meaning of the names

No stipulation required.

3.1.3. Use of pseudonym

Where pseudonyms are used, this is controlled by the corresponding Certification Policy.

3.1.4. Interpretation of name formats

The Consorci AOC complies in any case with what is established by the reference X.500 standard in ISO / IEC 9594, as well as by RFC 5280 and by the CA / Browser-Forum Requirements (Baseline Requirements and EV Guidelines).

3.1.5. Uniqueness of names

Certification Authority issues different types of certificates. Certificate subscriber names are unique for every certificate generation service operated by the Certification Authority and for every type of certificate. An individual may only hold one of each different types of certificate issued by the Certification Authority. Values CIF or NIF are used for distinguishing two entities in case of name duplicity problem.

It is not possible to assign a subscriber name that has already been used by another subscriber.

All staff associated to the Register Authority have as essential requirement to attend a training course imparted by the Certification Authority.

3.1.6. Sequencing and frequency of labour rotation

No stipulation required.

3.1.7. Resolution of conflicts related to names

Consorci AOC will not arbitrate in cases of name disputes and will have no responsibility in this respect. Assignment of names will be done based on sequential order.

Regarding the treatment of registered trademarks, please see section 9.5.3.

3.2. Initial identity validation

3.2.1. Private key possession test

When a certificate is issued in a hardware device, the private key is created the moment before certificate generation, via a procedure that guarantees the confidentiality and association with the identity of the applicant.

Every Register Authority is responsible for guaranteeing the device delivery and access for the applicant in a secure way. In other cases, the method of private key possession test by the subscriber will be the delivery of PKCS#10 or an equivalent cryptographic proof, or otherwise via a method approved by Consorci AOC.

3.2.2. Authentication of organisation identity

Register Authority must verify the following data in order to authenticate the organisation identity:

- Data related to the organisation company name
- Data related to the subscriber constitution and legal personality.
- Data related to the scope and validity of the applicant representative capacity
- Data related to the organisation tax identification code or equivalent.

Consorci AOC reserves the right not to issue the certificate if considers that the submitted documentation is not sufficient or adequate for the verification of this data.

3.2.2.1. Register Authority

Certification Authority authenticates for any Register Authority component, prior to a certificate issuance and delivery, Authority and operator identity according to the corresponding section of this CPS.

3.2.3. Authentication of a natural person identity

This section contains information for the verification of a natural person identified in a certificate.

3.2.3.1. Identification elements

Number and type of necessary documents required to confirm key holder identity are those accepted by Consorci AOC, as described within its regulations.

These identifying documents will contain at least:

- Full name 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 foreigners certificates)
- Date and place of birth.
- Other supporting information that can be useful for differentiating one person from another within the Institution scope (for example: photograph, email address, position, etc.).

3.2.3.2. Validation of identification elements

No additional stipulation required.

3.2.3.3. Necessity of personal presence

The identification of the natural person who needs a qualified certificate (the key holder), can be confirmed by:

- Their presence in front of those enabled to verify their identity
- The procedure that the administrative regulation establishes, when the appearance is conducted towards Public Administrations.
- The videoconference identification method may be used only in those cases allowed by Spanish legislation, according to article 24.1.d) of Regulation (EU) Nº 910/2014. The validity of the certificates issued through this identification method and its use will be limited as established by current legislation at all times.

Before the issuance and delivery of a qualified certificate, the Certification Authority - via Register Authority intervention - will need to confirm the identity of the key holder by way of their appearance.

The appearance may differ to the certificate delivery and acceptance moment. Identity of the person to be the private key holder may be validated then during the appearance.

The requirement for appearance can be removed if the dispatch request has been authenticated using an electronic certificate of qualified signature classified by Consorci AOC, only when it is in force and the previous validated personal presence is not older than five years.

In the case of certificates for citizenship, personification can be dispensed with if the signature contained in the request to issue a certificate has been notarized and in the cases provided

for in article 24 of Regulation (UE) nº 910/2014.. But this CPS does not support this mechanism for the lack of existence of an effective procedure on behalf of the notaries.

3.2.3.4. Connection between natural person and organisation

Regulated differently in every Certification Policy in force for every type of Certificate.

3.2.4. Domain validation

To guarantee that an applicant entity has control over the domain (URL) they ask to include in a certificate, the following checks are made:

- **Organisational**: domain name ownership is requested, certified by a legal representative of the organisation, apart from the legal person name for who the certificate is issued, and the register number when it is appropriate, as it is described within the official registers.

- **Technical**: the following whois authenticated services are consulted:

    - for "*.es" domains: https://www.nic.es/sgnd/dominio/publicInformacionDominios.action

    - For other domains:

      Consult http://www.iana.org/domains/root/db/ which is the WHOIS server authorised for searching information regarding the domain, depending on the Top-Level Domain (TLD), meaning if the domain ends with .com, .org, .net, ...

- **Domain register validation: a**n email is sent to the domain registrant address and/or to an addresses such as "admin", "administrator", "webmaster", "hostmaster" or "postmaster" followed by @ and the name of the authorisation domain, with a random unique number that must be replied within 30 days.

3.2.5. Information not verified

The Certificate Authority is responsible for all 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).

However, certificates may include non verified information, for example the email address, provided that end users are notified of this fact within the certificate or the corresponding legal instruments.

All the information on the SSL certificates is verified prior to their issuance, contrasting with independent information sources.

3.2.6 Interoperability criteria

No stipulation required.

3.3. Identification and authentication of 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

3.3.2. Validation for certificates renewal after revocation

Certificates renewal after revocation is not possible.

4. Operational features of certificate life cycle

4.1. Request for certificate issuance

4.1.1. Legitimacy of a request to issue

The requirements that an applicant must fulfill will depend on the type of requested certificate and will be described in the CP for every type of certificate.

4.1.2. Registration procedure; responsibilities

The Certification Authority, prior to a certificate issuance, assures that the certificate requests are completed, accurate, and duly authorised.

Before a certificate issuance and delivery, the Certification Authority will inform the subscriber or the key holder about terms and conditions applicable to the certificate. This requirement is met via legal instrument delivery that connects the Certification Authority with the subscriber, or via delivery receipt to the key holder, which will contain the referred information. This information will be communicated on paper or electronically, and in simple language.

4.2. Certification request procedure

The requirements that a certification request must have will depend on the type of the requested certificate and will be described within the CP for every type of certificate.

4.3. Certificate issuance

4.3.1. Certification Authority actions during the issuance process

For every certificate request processed, the Certification Authority:

- Utilizes a procedure of certificates X.509 v3 generation that associates the certificate with the register information in a secure way, including the certified public key, via digital signature of the Certification Authority.
- Protects the confidentiality and integrity of the register data.
- Includes within the certificates the information established in the applicable legislation described in section 9.15 Conformity with the applicable law.
- Fulfills the obligations established within the corresponding legislation, in the case of qualified certificates generation.
- Meet the controls established within this CPS.

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

4.3.2. Communicating the subscriber about the issuance

The Certification Authority communicates the subscriber of the certificate issuance, or the corresponding incident. Similarly, it will indicate the availability of the certificate and the form in which it can be obtained.

4.4. Certificate acceptance

4.4.1. Responsibilities of the Trust Service Provider

The Certification Authority (or TSP):

- If it is not been done before, and when needed, will confirm the subscriber identity if not confirmed before.
- Will provide the subscriber with access to the certificate.
- Will deliver, if required, the signature cryptographic device, signature verification, coded or not.
- Will provide the following information:
    - Basic information about the policy and the use of the certificate, particularly including information about the Associated Certification Authority and the applicable CPS, as well as its obligations, faculties and responsibilities.
    - Information about the certificate and the cryptographic device.
    - Recognition of the holder receiving the certificate, and if need be, the cryptographic device, and the acceptance of both referred elements.
    - Key holder obligations.
    - Key holder responsibilities.
    - Exclusive imputation method to the private key holder and their certificate or cryptographic activation data, according to the corresponding sections in this CPS.
    - Date of the delivery and acceptance.

4.4.2. Conduct which constitutes the certificate acceptance

The certificate is accepted via signature of the holder certificate delivery or the key custody responsible.

It can also be accepted via telematic mechanism for certificate activation.

4.4.3. Publication of the certificate

Certificates can be published without previous consent of the key holders.

Certificates may be published if the specific consent of the individuals is available, the data of which are included in the aforementioned certificates.

4.4.4. Notifying the issuance to third parties

No stipulation required.

4.5. Use of the key pair and the certificate

4.5.1. Use for key holders

No stipulation required.

4.5.2. Use for third parties that trust certificates

No stipulation required.

4.6. Certificate renewal without keys renewal

Certificate renewal without key renewal is not allowed.

4.7. Certificate renewal with keys renewal

Certificate renewal starts 2 (two) months before the certificate expiration date, when the subscriber receives an email to inform on required steps to follow to execute the certificate renewal. This email is sent again 30 (thirty) days before the expiration.

The certificate renewal process is same as for new certificate issuance. When a renewal is requested, the Inner Register Authority must verify that the registration data is still the same, and any data that has changed must be verified, evidence of this verification must be kept and the subscriber must agree with the modification, as specified in the corresponding section in this CPS.

However, if it is been more than five years since the subscriber was identified in person in a Register Authority office, they will have to attend in person again to renew.

The Register Authority will inform the key holder of the legal conditions related to the provided service, as is done in the process of issuance of new certificates.

For individual certificates in keychain support, the subscriber will have to present at the Register Authority office, since new keys will be generated in this device.

4.7.1. Telematic renewal

The Register Authority allows telematic renewal of digital certificates - based on a secure authentication and the corresponding electronic signature of the delivery form or the new certificate issuance request made with the certificate that needs to be renewed within the last two months of validity - as long as the last time the key holder identified in person in an Register Authority office was not more than five years ago.

4.8. Modification of certificates

Modification of certification data requires revocation and issuance of a new certificate. To all effects, the modification is considered a revocation.

When the subscriber acknowledges changes within the mandatory information or related to position, use limitations or user devices of the certificates (for example IP addresses or server/application data), or requires the modification of other data included in the certificate (email address, etc.) they will be able to manage the renewal of the current valid certificate. In certain cases, depending on the information that needs to be modified, this revocation can be made after a certificate issuance with the updated data.

The Register Authority will require the accreditation of the modification justifying conditions.

4.9. Revocation and suspension of certificates

4.9.1. Causes of certificate revocation

The Certification Authority will be able to revoke a certificate by the concurrence of the following causes:

1. Circumstances affecting the information contained in the certificate
    - Modification of any data contained in the certificate.
    - Discovery of that some data provided in the certificate request is not correct, as well as alteration or modification of the circumstances verified for the certificate issuance.
    - Discovery of that some data contained in the certificate is not correct.
2. Circumstances affecting certificate private key security
    - Breach of the private key, infrastructure or Certification Authority system that issued the certificate, as long as it affects the reliability of the certificates issued since this incident.
    - Certification Authority infraction of the requirements described within the management certificates procedures established within the CP of the Certification Authority.
    - Breach or suspicion of breach of the key security or the key holder certificate security.
    - Non authorised access or use of the private key of the key holder by third parties.
    - The irregular use of the certificate by the key holder, or lack of diligence in the private key custody.
    - The CA knows of a proven method that can easily calculate the subscriber's private key based on the public key in the certificate
3. Circumstances affecting the cryptographic device security
    - Breach or suspicion of breach of the cryptographic device security.

- Loss or deactivation due to cryptographic device damage.
- Non authorised access by third parties to activation data of the key holder.

4. Circumstances affecting the key holder.
    - Finalisation of the relationship between the Certification Authority associated to the key holder.
    - Modification or extinction of the underlying legal relationship or the cause that motivated the key holder to issue a certificate.
    - Certificate applicant infraction of the established requirements for their request..
    - Key holder infraction of their obligation, responsibilities and guarantees, established in the corresponding legal instrument or the CPS of the Associated Certification Authority that issued the certificate or the corresponding CP.
    - The disability or death of the key holder.
    - In cases of corporate certificates, the extinction of the certificate subscriber legal person, as well as the finalisation of the subscriber authorisation to the key holder, or the finalisation of the relationship between the subscriber and the key holder.
    - Subscriber request of certificate revocation, as established in section 3.4. of this statement.
5. Circumstances related to Extended Validation certificates:
    - Subscriber request of certificate revocation.
    - The Certification Authority obtains reasonable proof that there is a breach in the subscriber private key or the certificate has been stolen by a third party.
    - The Certification Authority is notified from a tribunal or an arbitrator about the revocation of the right to use the domain name that appears in the certificate, or knows of the impossibility of the domain renewal.
    - The Certification Authority acknowledges unfulfillment of PKI Disclosure Statement for electronic certificates (PDS) or other specifications established in the operative legal documentation.
    - The Certification Authority ceases support activities for Extended Validation certificate revocation or loses the right to issue Extended Validation certificates. If the Certification Authority may guarantee the maintenance of CRL and OSCP (Online Certificate Status Protocol) validation services, revocation is not necessary.
    - Breach or suspicion of breach of any top level hierarchy Certification Authority keys.
    - Revocation of publication of policies related to Extended Validation certificates.
    - Notification of the inclusion of a subscriber in the prohibited subscribers list (also blacklists made for victims of phishing or inverse engineering activities.
6. Other circumstances:

- Suspension of a digital certificate for a period of more than 120 days.
- The finalisation of the Associated Certification Authority service.
- The finalisation of the service provision by the Certification Authority.
- Legal or administrative resolution that orders the revocation.
- Compliance with the provisions of the current legal set of provisions.
- In the case of SSL certificates, for any of the causes established in the Basic Requirements of the CA Browser Forum (Baseline Requirements) and in the EV Certificates Guides (EV Guidelines) of the CAB-Forum and in the times established for each cause.
- Any circumstance established in Mozilla's Certificate Policies (Mozilla Root Store Policy)

The legal instrument that connects the Associated Certification Authority to the subscriber will establish that the subscriber must request the certificate revocation in case of acknowledging any prior described circumstances.

If the Associated Certification Authority does not have all the required information to determine a certificate revocation but has indication of its breach, it could decide to suspend.

4.9.2. Legitimacy of requesting a revocation

They will be able to request a certificate revocation:

- In cases of individual certificates, the subscriber on whose behalf the certificate was issued.
- In cases of corporate certificates, the authorised person for the subscriber entity; on occasion at the request of the key holder.
- The Register Authority that requested the certificate issuance.

4.9.3. 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 the exceptional case of unavailability of the telematic channel. It must to contain enough information to reasonably identify - under Certification Authority criteria - the certificate that is requested for revocation, and the authenticity and authority of the applicant. The detailed procedure is available on the Consorci AOC website.

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 of the Certification Authority, which is available 24x365. The contact details of the User Service Department are described in point "1.5.2. Organisation contact data".

Revocation action is made by one of the operators of the Register Entity, by accessing the web application and authenticating through a digital certificate issued by the Certification Authority.

Once the status change has been registered in the Certification Authority system, a new 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 applicable legislation.

4.9.4. Term time for revocation request

Revocation requests must be sent as soon as possible once the cause of the revocation is known.

Outside of the Authority Register office hours, the subscriber may request precautionary suspension of the certificate through the User Service Centre of the Certification Authority, according to the procedure defined on the Consorci AOC website.

4.9.5. Maximum term for revocation request process

When a Register Authority or Associated Certification Authority receive a revocation request, it will be processed as soon as possible, within 24 hours of receipt.

Before proceeding to a certificate effective revocation, the request addressee must authenticate it according to the requirements established in the corresponding section of this CPS.

When the revocation request has been sent to a Register Authority, they will be able to authenticate it, revoke the certificate directly or send a request to this effect to the Associated Certification Authority.

Also, the key holder must be notified about status changes of the revocated certificate. In cases of corporate certificates, the subscriber must be notified.

4.9.6. Obligation to consult information related to certificate revocation

Verifiers check the status of those certificates they want to trust in.

In order to verify the status of certificates it is necessary to consult the CRL in force by the Certification Authority that issued this certificate, or to consult an online service that gives

certificates status (OCSP Service or other certificate validation services) operated by a trusted validation services provider.

Certification Authorities that form the certification hierarchy operated by Consorci AOC publish freely the information about status of certificates issued by them. The URLs where this information is published (CRL lists and OCSP services), are indicated within the content of the certificates they issue.

The Certification Authority provides information to the verifiers about how and when to find the corresponding CRL.

4.9.7. Frequency of the Certificate Revocation List (CRL) publication

The Root Certification Authority will issue a Authority Revocation List (ARL) at least every six months, or extraordinarily, when the revocation of a certificate of authority occurs.

Each subordinate Certification Authority will issue a CRL daily, and in an extraordinary manner, within 30 minutes of each time a certificate is suspended or revoked. The validity of this CRL will be 7 days. The CRL does not contain state information from the expired certificates.

4.9.8. Maximum period for CRL publication

Once they are generated, new versions of CRL are published immediately on Consori AOC website and via the URLs indicated within the content of the issued certificates.

4.9.9. Availability of certificate status check services

Verifiers of digital certificates may consult the online service that provides certificate status (*OCSP responder* service, for online certificate status query, or other certificate validation services) operated by a trusted validation services provider.

Consorci AOC offers a free OCSP responder service to check the status of the certificates issued by the Certification Authorities that form the certification public hierarchy of Cataluña.

The URL of this service is indicated within the content of the issued certificates. This information related to the OCSP profile, and in general to the service function, can be found at http://www.aoc.cat/catcert/regulacio.

In case of cessation of the activity and / or compromise of the EC keys, a last CRL will be generated that will be kept intact and available for consultation, guaranteeing the availability of the information service on the status of the certificates, for at least 15 years since its publication.

The provision of information on the status of revocation of the Certificates, in the event of cessation of activity of the Consortium AOC as a TSP, is guaranteed by transfer, to the supervisory body or to another Provider with which the corresponding one is reached. agreement, of all the information related to the Certificates and, especially, of the data of their revocation status.

4.9.10. Obligation to consult information regarding certificate status check services

Verifiers check the status of those certificates they want to trust in. There is no stipulation related to the mechanism used for the status check.

4.9.11. Other forms of certificate revocation information

No stipulation required.

4.9.12. Special requirement for private key security breach cases

The breach of an Associated Certification Authority private key will be communicated, as far as possible, to all participants of the certification public hierarchy of Cataluña, including at least in the corresponding CRL the reference to the digital certificate of this Certification Authority.

Additionally, Third Parties may use the following methods to demonstrate a possible key compromise:

- Send a signed CSR, the private key that has been compromised, or another challenge response signed by said Private Key and verifiable by the public key.
- Provide references to sources of security and / or vulnerability incidents for which the compromise is verifiable.
- Submit binaries that contain a compromised private key, including the method to extract the private key.

The Third Parties will notify said commitment to the CA via email for notification of incidents: incident_pki@aoc.cat

4.9.13. Causes of certificate suspension

The Associated Certification Authority will suspend a certificate in the following cases:

- In those cases legally provided by the electronic signature and trusted digital services applicable regulation, and in any case when a legal or administrative resolution orders it.
- When the required documentation for the revocation request is sufficient , but it is not possible to reasonably identify the key holder.
- When the required documentation for the revocation request is not sufficient, even if it is possible to reasonable identify the key holder.
- When the required documentation for the revocation request is not sufficient, and it is not possible to reasonably identify the key holder.
- When the certificate is not activated in a period of more than 120 days since its issuance.
- If there is a suspicion of a key breach, and until it is confirmed. In this case, the Associated Certification Authority must make sure that the certificate is not suspended for more time than necessary to confirm the breach.

Suspension is prohibited for the following device certificates, which may only be revoked:

- Secure Socket Certificate (Dispositiu SSL)

- Secure Socket Certificate Extended Validation (Dispositiu SSL EV)
- Electronic Office Certificate (Seu-e nivell mig/substancial)

4.9.14. Effect of certificate suspension

It will be considered that the actions during a certificate suspension period are not valid, as long as the certificate is eventually revocated. But if the suspension is lifted (activation) and the certificate becomes valid again, the actions during the suspension period will be considered valid.

Suspension is reversible up to a maximum of a 120 day since the date of suspension, while after that time, if the activation has not been requested, it will become automatically revoked.

To perform the activation of a suspended certificate, the key holder must attend in person to the Register Authority that approved the issuance request of this certificate, and present the verifying document of their identity for the Register Authority to confirm.

Certificate status changes (suspension, enabling, etc) must be informed to the key holder, and in cases of personal certificates for public sector, changes must be informed to the subscriber.

4.9.15. Who can request a suspension

Suspension of a certificate may be requested by:

- In cases of individual certificates: the key holder the register authority that requested the certificate issuance, acting their name.
- In cases of corporate certificates: an authorised representative of the subscriber entity, the register authority that requested the certificate issuance, or the key holder.

4.9.16. Procedures of suspension request

The procedure of suspension may be processed as follows:

1. By the key holder, calling the User Support Centre of the Certification Authority.
2. In cases of corporate certificates, by the certificate subscriber entity calling the User Support Centre of the Certification Authority.
3. By the Register Authority. In cases when the Register Authority is authorised to do so by the Certification Authority, then the Register Authority will be able to process the suspension. Otherwise the suspension is processed by the Certification Authority.

To initiate a suspension the following information is required:

- Date and time of the suspension request.
- Full name of the key holder whose digital certificate is to be suspended.
- Id Document of the key holder whose digital certificate is to be suspended.
- *SerialNumber* of the certificate to be suspended.

- Detailed reason for suspension request.
- Suspension code associated to the certificate, or by default, secret question and response chosen at the time of activation.
- In cases of corporate certificates:
    - Identity of the subscriber who requests the suspension (in case this is not the same holder).
    - Contact information of the Institution that requests the suspension.
    - Body and department to which the key holder is associated to.

Once the validity of a certificate is suspended, the subscriber will be informed, and where appropriate, the key holder, regarding the suspension status and the maximum suspension period of 120 (one hundred twenty) calendar days.

4.9.17. Maximum suspension period

The maximum suspension period will be 120 (one hundred twenty) calendar days.

4.9.18. Reactivating a suspended certificate

To reactivate a suspended certificate, the subscriber must present and identify in front of the Associated Certification Authority, through the Register Authority that approved the certificate request, and sign the corresponding reactivation document request to record the reason that caused the suspension.

4.9.19. Validity period of certificates

Validity period of certificates will be indicated within the certificate itself, up to a maximum of 5 years.

4.10. Certificate status check services

4.10.1. Operational features of the services

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

Additionally, the verifiers shall be able to enquire on the published certificates in the directory of the Certification Authority.

The CRLs does not contain the status information the expired certificates. However, in case of request about the status of an expired certificate, the valid information will be the one that provided the verification system in line of status certificate (OCSP).

4.10.2. Availability of the services

Verifiers of digital certificates may consults an online service that provides certificate status (*OCSP responder* service, for online certificate status query, or other certificate validation services) operated by a trusted validation services provider.

Consorci AOC offers a free *OCSP Responder* service to check the status of the certificates issued by the Certification Authorities that form the certification public hierarchy of Cataluña.

The URL of this service is indicated within the content of the issued certificates. This information related to the OCSP profile, and in general to the service function, can be found at http://www.aoc.cat/catcert/regulacio.

CRL and status certificate online enquiry systems will be available 24x7.

In case of failure of certificate status checking system due to causes beyond the Certification Authority control, then the Authority will use reasonable efforts to ensure that the service is resumed as soon as possible.

4.10.3. Other functions of the services

No stipulation required.

4.11. End of the subscription

The end of the subscription will not imply revocation of certificates that have been issued, they may continue to be used until they expire.

4.12. Key deposit and recovery

4.12.1. Policy and practices of key deposits and recovery

The possibilities for a Certification Authority to provide key deposit and recovery services to one or more categories of certificates must be contained (in case this option is possible) in the corresponding CP. Also in this policy the following aspects must be detailed:

a. Who can request deposit and key recovery

b. How the request should be processed

c. Requirements of requests confirmation

d. Mechanisms used to deposit and recover keys

4.12.2. Policy and practices of session keys encapsulation and recovery

No stipulation required.

5. Controls of physical, management and operational security

The Certification Authority ensure the application of adequate administrative and management procedures according to the recognised standards, in particular:

a. A risk management analysis is made to evaluate required security measures.

b. The Certification Authority must be responsible for providing services in a secure way, even if parts are subcontracted. Third parties responsibilities are defined and the required legal controls must be established to guarantee that their obligations are accomplished with an equivalent security level.

c. The Certification Authority establishes the main rules regarding security via a high-level body that defines the information security policy of the Entity and gives the necessary publicity via action of internal communication.

d. The Certification Authority maintains the necessary infrastructure to manage the security of operations. Any change that has impact on the security level must be approved by the body referred previously.

e. The Certification Authority implements and maintains security control and operational procedures of the facility, the systems and the active data on which the provision of the service is based.

f. In case of total subcontracting of the services, the Certificate Authority guarantees the maintenance of the necessary security level.

5.1. Control of physical security

5.1.1. Secure areas

The Certification Authority has premises that physically protect the provision of at least the services of certificates and cryptographic devices generation, revocation management, and against breach caused by non authorised access to systems or data.

Physical protection is obtained via creation of security perimeters clearly defined around the services of certificates and cryptographic devices generation and revocation management. Those parts of the facility that are shared with other organisations are outside of these perimeters.

5.1.2. Physical security controls

The Certification Authority establishes physical and environmental security controls to protect the premise resources where systems installations are located, same systems and equipment used for operations. The physical and environmental security policy applicable to services of certificates and cryptographic devices generation and revocation management establishes prescriptions for the following contingencies:

- Physical access control
- Protection against natural disaster.

- Fire precaution measures.
- Errors in support systems (electrical supply, telecommunications, etc.).
- Building demolition.
- Flooding
- Anti-theft protection.
- Conformity and non authorised access.
- Disaster recovery.
- Non authorised removal of equipment, information, supports and applications related to components utilised for the Certification Authority services.

5.1.3. Facilities location and construction

Facilities location allows the attendance of security forces immediately after the notification of an incident.

Quality and strength of construction materials of the facilities guarantee adequate levels of protection against forced entry.

5.1.4. Physical access

The Certification Authority establishes security levels with restricted access to the different perimeters and defined physical barriers.

To access the facilities of the Certification Authority where certificate life-cycle processes are managed, previous authorisation and date, time and registration of access are necessary, including close circuit television recording and archiving.

This identification towards the access control system is made via recognition of a biometric parameter of the individual, except in cases of escorted visits.

The management of the cryptographic keys, as well as its storage, is done within the specific facilities and requires access and permanency double controls.

5.1.5. Electricity and air conditioning

The Certification Authority IT equipment are duly protected against electrical power surges or cuts that could damage or interrupt the service.

The facilities rely on electrical supply stabilisation system, as well as on a system that generates sufficient uninterrupted electrical supply for the time required to close the systems in an organised and completed way.
The IT equipment is located in an environment where climate control is guaranteed for the optimal conditions for their operation.

5.1.6. Water exposure

The Certification Authority has flood detection systems adequate to protect the equipment and assets, in case of facilities location conditions make this necessary.

5.1.7. Fire warning and protection

All the facilities of the Certification Authority rely on detection and extinction automatic systems.

In particular, cryptographic devices and supports that store keys of the Certification Authorities will also utilise specific and additional fire protection system.

5.1.8. Removable data storage

Usage of removable storage supports is minimised and restricted uniquely to file movement between systems via USB pendrive devices. To guarantee both integrity and confidentiality, removable storage supports will be stored in a safe in the same room.

5.1.9. Waste management

Secure elimination, both paper and magnetic waste is managed via mechanisms that guarantee the impossibility of information recovery.

In the case of magnetic media, they are formatted, permanently deleted or physically destroyed.

In the case of paper documentation, it is submitted to a physical destruction treatment.

5.1.10. Secure offsite copy

Secure copies of information systems are held in facilities that are physically separated from where the IT equipment is maintained.

Secure copies are made online within the contingency system, an alternative CPD, through encrypted communications.

5.2. Control procedures

The Certification Authority guarantees that its systems operate in a secure way by establishing and implementing procedures for the related functions that affect service provision.

The Certification Authority personnel execute the administrative and management procedures according to the Certification Authority security policy.

5.2.1. Reliable functions

Persons that occupy these positions are formally appointed by the high management of the Certification Authority.

Reliable functions include:

- Personnel responsible of the security
- System administrators
- Systems operators
- Registration operators

- System auditors.
- Any other person with access to personal data.

According to rules ETSI EN 319 401 and CEN/TS 419261, the following roles must be established:

- Security Officer: global responsible for administration and implementation of the security policies and procedures.
- Registration Officer: Responsible to approve, issue, suspend and revoke end-entity certificates, as well as adequate verification on certificates of website authentication.
- Revocation Officers: responsible to implement changes to the certificate status.
- System Administrator: authorised to implement changes within the system configuration, without access to data of the system.
- System Operators: responsible for the system daily management (monitoring, backup, recovery…).
- System Auditors: authorised to access to systems logs and verify the procedures.
- CA Operator - Certification Operator: responsible to activate the CA keys in online environment, or the certified signature and CRL processes in the Root Offline environment.

5.2.2. Number of persons per task

The Certification Authority guarantees at least two people to do the tasks that require multi-person control and that are detailed below:

- The generation of the key of the CA'S.
- Recovery and backup of the CA's private key.
- The issuance of CA's certificates.
- Activation of the CA's private key.
- Any activity performed on hardware and software resources that support root CA.

5.2.3. Identification and authentication for each function

The Certification Authority identifies and authenticates personnel prior to their accessing of the corresponding reliable function.

5.2.4. Roles which require task separation

The Certification Authority identifies, within its security policy, reliable functions or roles:

Reliable functions include:

a. Security Officer
b. Registration Officer
c. System Administrator
d. System Operators
e. System Auditors
f. Any other person with access to personal data.

The following restrictions apply in all cases:

1. Person acting as Security Officer or Register Officer cannot also act as System Auditor.

2. Person acting as System Administrator cannot also act as Security Officer or System Auditor.

Role descriptions must be constructed with the understanding that sensitive function separation is required, as well as a minimum privilege concession when possible. To determine the sensitivity of the function, the following elements must be taking into account:

a. Duties associated with the function
b. Access level
c. Monitoring of the function
d. Training and awareness-raising
e. Required skills

The referred restrictions are applied the following way:

- Person acting as Security Officer or Register Officer cannot act as System Auditor.
- Person acting as System Administrator may not act as Security Officer or System Auditor.

5.3. Personnel controls

The Certification Authority 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:

- Service Responsible

- The Certification Authority Responsible
- Security Responsible
- Operations Responsible
- Administration, Operation and Exploitation Technical Team
- Network Administrators
- Certification Authority users

In addition, regulation compliance extends to the following personnel:

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

5.3.1. Record, qualification, experience and authorisation requirements

The Certification Authority is formed by qualified personnel with the required experience to manage the offered services provision within the electronic signature scope and the appropriate security and management procedures.

This requirement will apply to personnel managing the Certificate Authority, specifically to those who are related to security personnel procedures.

Qualification and experience may be supplied via appropriate training.

Personnel in trust roles are free of personal interests that could be in conflict with other functions development.

The validation specialists for issuing web authentication certificates must meet the training and qualification prerequisites established in section 14.1.2 of the EV Guidelines and section 5.3.3 of the Baseline Requirements of the CA / Browser Forum.

5.3.2. Training requirements

The Certification Authority trains personnel to enable them to obtain the necessary qualification for trust and management roles.

Training includes the following contents:

- Security principles and mechanisms of the Catalunya Certification Public Hierarchy, as well as the user environment of the person to be trained.
- Hardware and software versions in use..
- Tasks that personnel need to complete.
- Process management of security breaches and incidents
- Business continuity processes.
- Security management procedure related to personal data handling.

The Certification Authority, moreover, provides appropriate information to all involved personnel in operations as Register Authority, including work and security procedures. A periodic training regarding security, contingency plans and incidents management is also given.

5.3.3. Requirement for and frequency of training update

All personnel related to Register Authorities require attending to the Register Authority training taught by Consorci AOC.

There will be annual basis updates, except for modifications in the CPS, which will be notified as soon as they are approved.

5.3.4. Penalties for unauthorised actions

The Certification Authority has a penalty system to determine responsibilities derived from non authorised actions.

Disciplinary actions include suspension and termination of the person responsible for the actions in question.

5.3.5. Requirements for hiring personnel

The Certification Authority hires professionals for all functions, including trust roles. In this case, they are subjected to the same controls as the other employees.

Given the case that a person does not need to be subjected to these controls, they are constantly accompanied by a trusted employee.

In the case that all or parts of certification services are operated by a third party, controls and precautions described in this section 5, or in other parts of the certificate policy or this CPS, are applied and completed by the third party that conducts the operational functions of the certification service. Consorci AOC is responsible, in all cases, for the effective execution.

These aspects remain under the legal instrument used to control the agreement for the services provision by a third party distinct from the Certification Authority.

5.3.6. Provision of documentation to personnel

The Certification Authority provides strictly necessary documentation to personnel as required in order to competently develop its functions

5.4. Procedures for security audit

5.4.1. Types of registered events

The Certification Authority keeps a register, as a minimum, of the following events related to the entity security:

- System start-up and shutdown.
- Start and stop of the application used for certification Authority (technical).
- Attempts to create, delete, change passwords or permissions of users within the system.
- Changes to the certificate Authority (technical) keys.
- Changes to certificate issuance policies.
- Attempts to enter and leave the system.
- Non authorised attempts to enter the Certification Authority network.
- Non authorised attempts to access system files.
- Certification Authority keys generation.
- Invalid attempts at reading and writing in a certificate and in a directory.
- Events related to certificate life-cycle, such as request, issuance, revocation, and renewal.
- Events related to cryptographic module life-cycle, such as reception, use and deinstallation.

The Certification Authority also keeps ,either manually or electronically, the following information:

- Key generation and database management ceremony.
- Physical access registers.
- Maintenance and changes to system configuration.
- Personnel changes.
- Discrepancy and error reporting
- Register of material destruction containing information regarding keys, activation dates or subscriber personal information.
- Activation data possession for operations with the Certification Authority private key.
- Reporting on attempts of physical intrusion into the facilities that support certificates issuance and management.

5.4.2. Treatment frequency of audit registers

Audit registers are examined at least once a week for searching suspicious or non habitual activity.

Processing of these registers processing consists of revisions that include verification that the registers themselves have not been manipulated, a brief inspection of all register entries and a deeper investigation of any alert or irregularity within the registers. Actions taken resulting from the audit are also documented.

5.4.3. Preservation period of audit registers

Audit registers are retained during at least 2 (two) months after processing and then archived according to section 5.5 of this CPS.

5.4.4. Protection of audit registers

Register files, either manual or electronic, are protected from reading, modifications, deleting or any other type of unauthorised manipulations via both logical and physical controls.

5.4.5. Procedures for maintaining secure copies

Incremental support copies of audit register are generated daily and complete copies on a weekly basis.

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

Accumulation system of audit registers is an internal system of the Certification Authority formed by the application registers, the networking registers, the operating system registers, and manually generated data, that authorised personnel store.

5.4.7. Notification of audit events to the event originator

When the accumulation system of audit register records an event, it is not necessary to send a notification to the individual, organisation, device or application that caused the event.

It is communicated whether the result has been successful, but not that the action has been audited.

5.4.8. Analysis of secure vulnerabilities

Events arising from the audit process are stored, among other reasons, for monitoring system vulnerabilities.

Analysis of internal vulnerabilities are conducted at least quarterly while external reviews are conducted annually.

5.5. Archive of information

The Certification Authority guarantees that all information related to certificates is stored during an appropriate period according to section 5.5.2 of this CPS.

5.5.1. Types of registered events

The Certification Authority maintains a register of all the events that occur during a certificate life cycle, including its renewal.
The Certification Authority registers the following:

- Type of document provided in the certificate request
- Unique identification number provided by the aforementioned document
- Identity of the Register Authority that accepts the certificate request
- Location of certificate request copies and agreement signed by the subscriber, in case of individual certificates.

The Certification Authority must also preserve the following original documents:

- Certificate request form
- Data certificate
- Delivery form of the certificate subscriber

5.5.2. Register preservation period

The Certification Authority maintains the registers specified in section 5.5.1 during a 15 (fifteen) year retention period, initiated from the time of certificate expiration or the end of the service provided.

All information related to Infrastructure Certificates is permanently stored.

5.5.3. Archive protection

The Certification Authority assures correct protection of archives via assignment of qualified personnel towards handling, storage in fire-resistant boxes and external installations in required cases. The Certification Authority will use the necessary means to guarantee the confidentiality of digital signature private key against third parties during the generation.

5.5.4. Support copy procedures

A communication technical worker from the Certification Authority is responsible for making secure copies of logic access logs to Registration Authority 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.

Also, secure copies of KeyOne application customised for the Certification Authority are created. These copies are stored by the Certification Authority within its facilities.

5.5.5. Requirement for date and hour seal

The Certification Authority issues certificates and CRLs with date and hour information.

5.5.6. Location of archive system

The Certification Authority has a storage system for archive data outside of its own facilities.

5.5.7. Procedures for obtaining and verifying archive information

Only personnel authorised by the Certification Authority have access to archive data, whether stored within their own facilities or to the records of the Registration Authorities.

5.6. Key renewal

The Certification Authority renewed certificates are communicated to end users through their publication in Consorci AOC directory.

5.7. Key security breach and disaster recovery

5.7.1. Procedures for incident and security breach management

The Certification Authority establishes the procedures that apply to incident management affecting keys, and specifically, to breaches in the security of these keys.

5.7.2. Resources, application or data corruption

When a resources, application or data corruption event occur, the Certification Authority starts the necessary management according to Security Plan, Emergency Plan and Audit Plan, to bring the system back to normal functioning state.

5.7.3. Security breach of the Entity private key

The Business Continuity plan of the Certification Authority (or disaster recovery plan) considers as a disaster the Certification Authority private key breach or suspicion of breach In case of breach, the Certification Authority will inform all subscribers and verifiers.

- Inform all subscribers and verifiers of the commitment
- Will indicate that certificates and revocated status information delivered using the Certification Authority private key are not valid anymore.
- Will revoke, within the period agreed with the national supervisor, the certificates issued by this CA, if appropriate, Cessation Plan or Business Continuity Plan.
- Notify the national supervisory Body within a maximum period of 24 hours after having knowledge of the compromise of the private key.
- Notify the software manufacturers that trust the certificates, within the terms established in their respective CA admission policies.

5.7.4. Disaster on the facilities

The Certification Authority develops, maintains, tests, and if necessary, executes an emergency plan towards the facilities in case of disaster, either natural or man-made, indicating how to restore information system services. The location of the disaster recovery system has security physical protections described within the Security Plan.

The Certification Authority is able to restore PKI normal operations within 24 hours after the disaster, and may execute, as a minimum, the following actions:

- Certificates revocation
- Revocation information publication

Disaster recovery database used by the Certification Authority is synchronized with production database within time limits described in the Security Plan. Certification Authority disaster recovery equipment has the physical security measures specified in the Security Plan.

5.8. Service end

5.8.1. The Certification Authority

The Certification Authority makes sure that possible interruptions to subscribers and third parties are minimum as Certification Authority service cessation consequence, and particularly, assures a continuous maintenance of the required registers to provide certification evidence in legal processes.

Prior to ceasing services, the Certification Authority will execute, as a minimum, the following procedures:

- To inform all subscribers and verifiers (Certification Authority having any prior relationship with third parties is not required).
- To finalise authorisations of subcontracting that act on behalf of the Certification Authority in the certificates issuance process.
- To execute the necessary tasks to transfer obligations of register information maintenance and event register archive, during indicated respective periods, to the subscriber and verifiers.
- To destroy the Certification Authority private keys.

The Certification Authority declares in its Termination Plan the previsions it needs to adopt in case of service end, including:

- Notification to affected entities with 2 (two) months notice before the effective service end.
- How to treat the revocation status of issued certificates still not expired.

The Certification Authority will transfer the certificates according to terms of the electronic signature and trusted digital services applicable legislation.

5.8.2. Register Authority

No l stipulation required.

6. Technical Security Controls

The Certification Authority 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 certificates

Public and private key can be generated for the future key holder or the Certification Authority.

6.1.2. Delivery to private key to the subscriber

For qualified signature and high-level certificates, the private key must be delivered to the subscriber duly protected via smartcard.

In cases of qualified signature and high-level certificates, the private key must be delivered to the key holder, duly protected via smartcard which complies with requirements for profile of qualified device of electronic signature creation, or is stored according to section 3.2.1. of this CPS. Additionally, access mechanisms must be delivered to the key holder.

6.1.3. Delivery of the public key to the certificate issuer

The public key delivery method to the Certification Authority used is PKCS #10, or another equivalent proof, or any other method approved by Consorci AOC.

6.1.4. Distribution of the Trust Services Provider public key

The Certification Authority key and the keys of Certification Authorities that are one level below in the certification public hierarchy of Catalonia, are communicated to the verifiers, guaranteeing key integrity and authenticating the origin.

The Certification Authority public key, which is the hierarchy root, is published in the Certification Authority directory in the form of a auto signed certificate, together with a declaration that refers to the fact that the key allows authentication to the Certification Authority.

Additional measures are established to trust the auto signed certificate, such as verification of digital fingerprint in the certificate.

Public key of the Certification Authority is published in the Consorci AOC website: https://www.aoc.cat/catcert/regulacio.

Users access to the directory to obtain the Certification Authority public key.

6.1.5. Key measures

Certification Authority keys are 2.048 bits.

The keys of all certificates issued by the Certification Authority are 2.048 bits.

6.1.6. Generation of public key parameters

No stipulation required.

6.1.7. Quality verification of public key parameters

Conducted in accordance with technical specification ETSI TS 102 176, indicating the quality of the electronic signature algorithms.

6.1.8. Generation of keys in IT application or equipment

The Certification Authority key pairs are generated used cryptographic hardware accomplishing the established requirements by the technical specification CEN CWA 14167 or equivalent anc according to ITSEC, Common Criteria EAL 4+ o FIPS 140-2 Level 3 or higher security level.

Key pairs for qualified signature T-CAT certificates subscribers must be generated in smart cards or cryptographic devices that comply with the requirements established in the technical specifications CEN CWA 14170 or equivalent.

The key pair of signature and high-level certificate subscribers must be generated in smartcard or cryptographic devices according to requirements established within protection profile for qualified device of electronic signature creation.

Key generation for other certificates can be made via IT applications.

6.1.9. Key use purposes

Consorci AOC includes KeyUsage extension in all certificates, indicating the permitted uses of the corresponding private keys and technically limiting the functionality of the certificate in X.509v3 compliant software.

6.2. Protection of private key

6.2.1. Protection modules of private key

6.2.1.1. Cryptographic module standards

Certification Authority private keys must be protected using cryptographic module meeting the requirements established in a protection profile, according to Common Criteria EAL 4+o FIPS 140-2 Level 3 or higher security level.

The key pair of signature and high-level certificate subscribers must be generated in smartcard or cryptographic devices according to requirements established within protection profile for qualified device of electronic signature creation

In the event that there is going to be a loss of qualification of any of the devices used by the Consorci AOC as QSCD, a search will be made for substitute suppliers of said devices, the use of said device will cease before the loss of qualification and customers will be notified of future loss of qualification to take appropriate action. In any case, Consorci AOC will revoke all current certificates that have been issued in those devices that have lost their qualification.

Private key protection for other certificates can be made via IT applications

6.2.1.2. Life-cycle of cards with integrated circuit

Cards with integrated circuit (also known as smart cards), are delivered in every new certificate issuance by the (collaborator or internal) Register Authority, or directly by Consorci AOC when acting as Virtual Register Authority.

For every new certificate issuance or renewal a new card is delivered, certificates are not loaded onto pre-used cards.

When Consorci AOC detects card errors or defects, the cards in question may be removed from use. In case of detecting isolated errors or defects, the card will be replaced, once the certificate has been revoked, and a new certificate will be issued within a new card that will be delivered to the subscriber without additional cost.

6.2.2. Control for more than one person over private key

Offline access to the Certification Authority private key must require participation of three (3) cryptographic devices (protected by access key) amongst five (5) devices.

Each one of these devices is the responsibility of a named person, who uniquely knows the assigned access key.

Each device is responsibility of a particular person, who is the only person aware of its access key. Access key is acknowledged uniquely by one person responsible for the device. No person acknowledges more than one access key. Also, a sealed envelope is delivered before a notary containing the activation key that the responsible of each device has written. These envelopes may be removed from the Notary custody by the responsible or authorised person (bringing authorisation signed by the responsible).

Cryptographic devices are stored in the Certification Authority facilities and an additional person for accessing is required.

6.2.3. Private key deposit

Certification Authority private keys are stored in fire-protected spaces and protected by double physical access controls.

6.2.4. Secure copy of private key

Certification Authority private keys are stored in fire-protected spaces and protected by double physical access controls.

6.2.5. Private key archive

Certification Authority private key must have a secure copy stored and recovered (if required) by personnel subjected to personnel trust policy. This personnel must be specifically authorised for these purposes.

Private keys must be maintained and used protected by a cryptographic device that accomplishes requirements established in a protection profile according to Common Criteria EAL 4+, o FIPS 140-2 Level 3 or higher security level.

When the signature private key abandons these devices, it has do be done in a coded way.

Security controls that have to be applied in the Certification Authority support copies will be of the same or higher level than those which apply to keys normally in use.

When keys are stored in a cryptographic module controlled by dedicated process, appropriate controls must be provided in order that the keys will never abandon the device.

Certificate private key copies will not be stored, except for cases where this possibility may exist according to the CP, when a key will be stored to guarantee data recovery.

6.2.6. Insertion of private key into cryptographic module

Certification Authority private key are stored in files coded with fragmented keys and on smart cards (from which they may not be extracted).

These cards are used to introduce a private key into a cryptographic module.

6.2.7. Storage of private key in the cryptographic module

Private keys are directly generated in the cryptographic module.

6.2.8. Activation method of private key

At least two persons are required to activate the Certification Authority private key.

For T-CAT certificates in smartcard, the subscriber private key is activated via introduction of PIN in the smartcard or cryptographic device.

For T-CAT certificates in smartcard, when the smartcard or cryptographic device is removed from a device reader, introduction of PIN will be necessary again.

For personal certificates, the subscriber private key is activated via introduction of PIN in the smartcard, or via introduction of activation data required for the cryptographic device or storage system.

6.2.9. Private key deactivation method

For T-CAT certificates in smartcard, when the smartcard or cryptographic device is removed from a device reader, introduction of PIN will be necessary again.

For personal certificates including qualified signature basic policy, when the smartcard is removed from a device reader, or the application using it ends the session, introduction of activation data will be necessary again.

For personal certificates including advanced signature basic policy, when the application using the certificate ends the session, introduction of signature activation data (PIN) will be necessary again.

6.2.10. Private key destruction method

Private keys are destroyed to prevent theft, modification, divulgation or non authorised use.

6.2.11. Classification of cryptographic modules

Certification Authority modules obtain or exceed EAL 4 of Common Criteria (ISO 15408) level with the increases determined in CEN CWA 14167 technical specification.

Associated Certification Authority modules must be certified with the level and increases specified in a protection profile, according to Common Criteria EAL 4+, o FIPS 140-2 Level 3.

Subscriber modules of T-CAT certificates in smartcard obtain or exceed EAL 4 of Common Criteria (ISO 15408) level with the increases determined in CEN CWA 14169 technical specification.

Subscriber modules of qualified electronic signature and high-level certificates must be certified with the level and increases specified in a protection profile for qualified device of electronic signature creation.

6.3. Other management aspects of the key pair

6.3.1. Public key archive

The Certification Authority archives public keys in accordance with the provisions of section 5.5.

6.3.2. Use period of public and private keys

Use periods of keys are determined by the certificate duration, and once passed they may no longer be used.

As an exception, private key used for decoding may continue to be used until after the certificate expiration.

6.4. Activation Data

6.4.1. Generation and installation of activation data

If the Certification Authority facilitates a qualified device for signature creation to the subscriber, the device activation data must be generated in a secure way by the Certification Authority.

6.4.2. Protection of activation data

In order to give maximum protection to activation data, the Certification Authority distributes the certificate elements in two different channels.

- First, the Responsible of the Register Authority delivers the key holder the following material:
    - The holder delivery form
    - A card with the certificates
    - Necessary software to use the card
    - Certificates delivery letter
- At the same time, and by email, the following certificate activation data is sent to the holder

In this way secure separation of data distribution is achieved.

6.4.3. Other aspects of activation data

No stipulation required.

6.5. IT security controls

6.5.1. Specific technical requirements for IT security

It is guaranteed that access to the systems is limited to individuals who should be authorised for such. In particular:

- The Certification Authority guarantees an effective administration of user access level (operator, administrator, as well as any user with system direct access), to maintain the system security, including management of user accounts, audit and modification, or opportune access denial.
- The Certification Authority guarantees that access to information systems and applications is restricted in accordance with the access control policy, as well as that systems provide sufficient control security to implement the segregation of functions identified in the Certification Authority practices, including function separation between security systems administration and operators. In particular, the use of system utility programs is restricted and closely controlled.
- Certification Authority personnel identify and recognise themselves prior to using critical applications related to certificate life-cycle..

- Certification Authority personnel are responsible and have to be able to justify their activities, for example, via events archive.
- Possibility of sensitive data revelation must be avoided via reuse of storage media (for example deleted files) that remain available for non authorised users.
- Security and monitoring systems allow fast detection, registration and action against non authorised or irregular access attempts to their resources (for example, via intrusion detection system, monitoring and alarms).
- Access to public information directories of the Certification Authority (for example, certificates or revocation status information) has an access control for modification or data removal.

6.5.2. Evaluation of IT security level

The IT applications of the Certification Authority and the Registration Authority are reliable, in accordance with CEN CWA 14167-1 and EN 319 411-2. technical specifications, and the degree of compliance is evaluated via IT security auditing in accordance with CWA 14172-2 technical specification and an appropriate protection profile, according to ISO 15408 or equivalent.

6.5.3. Frequency of revision of the configurations of the trustworthy systems

The maximum revision interval maximum revision interval between 2 versions of the configurations of the trust systems will be 1 (one) year.

6.6. Life-cycle technical controls

6.6.1. System development controls

An analysis of security requirements during the phases of design is made, and requirements specification of any component used in the (technical) Certification Authority and (technical) Register Authority is also created to guarantee that systems are secure.

Change control procedures are used for new versions, updates and emergency patches..

6.6.2. Security management controls

The Certification Authority guarantees that its operational management functions of cryptographic modules 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.

The Certification Authority must maintain an inventory of all IT assets and will classify them according to their protection requirements, in line with the risk analysis conducted.

Systems configuration will be audited on a period basis, in accordance with the provisions established in the corresponding section of this policy.

Capacity requirements tracking will be done and procedures will be planned to guarantee sufficient system and storage availability for IT assets.

6.6.3. Evaluation of life-cycle security level

No additional stipulation required.

6.7. Network security controls

It is guaranteed that the access to the Certification Authority 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 the Certification Authority 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

No stipulation required.

7. Certificate profiles and certificate revocation lists

7.1. Certificate profile

The descriptive documents of digital certificate profiles that the Certification Authority issues are published on Consorci AOC website.

Certificates issued by Consorci AOC and Certification Authorities affiliate to Cataluña certification public hierarchy will have the contents and fields described within the corresponding “certificate profile“ document that Consorci AOC publishes on its website.

In any case, each certificate profile will include in its structure the following data:

a. Serial number, that will be a unique code in respect of the issuer distinguished name with an entropy greater than 64 bits.
b. Signature algorithm, some of which are identified in the corresponding section of this policy.
c. The issuer distinguished name, in accordance with the corresponding section of this policy.
d. Certificate validity start, in UTC, coded in conformance with RFC 6818
e. Certificate validity end, in UTC, coded in conformance with RFC 6818
f. The Individual distinguished name, in accordance with the corresponding section of this policy.
g. The individual public key, coded in conformance with RFC 6818
h. Generated and coded signature, in conformance with RFC 6818

Certificates will be in conformance with the following rules:

1. RFC 6818: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008
2. ITU-T Recommendation X.509 (1997): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework, June 1997
3. Specification “*Perfiles de Certificados Electrónicos*” produced by *Dirección de Tecnologías de la Información y las Comunicaciones* (DTIC) of *Ministerio de Hacienda y Administraciones Públicas* (MINHAP)

Additionally, qualified signature certificates will be in conformance with the following rules:

1. ETSI EN 319 412, sections 1, 2 and 5, of the version in force at the time of the publication of this policy.
2. Specification “Perfiles de Certificados Electrónicos” produced by Dirección de Tecnologías de la Información y las Comunicaciones (DTIC) of the Ministerio de Hacienda y Administraciones Públicas (MINHAP)
3. RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, 2001 (as long as it does not conflict with the previously referred TS 101 862)

Qualified certificates must also contain the following fields:

a. The indication that they are issued as qualified certificates

b. Certificate unique identifying code
c. Certification services provider identification that issues the certificate, indicating name or company name, address, email address and tax identification number.
d. Advanced electronic signature of the certification services provider that issues the certificate.
e. The signatory identification (the subscriber for cases of individual certificates, or the hey holder for cases of corporate certificates), via full name or National Id Document, or using a unique pseudonym.
f. Verification signature data corresponding to signature creation data that are under the signatory control.
g. Certificate use limitations, in case there are any
h. Transaction value limits for which the certificate can be used, in case they are established.

7.1.1. Version number

All certificates will contain a field with the version number, indicating that they are version 3 certificates.

7.1.2. Certificate extensions

The extensions for every certificate, as well as its semantic meaning, are described in the corresponding “certificate profiles” document that Consorci AOC publishes on its website.

7.1.3. Algorithm object identifier

The Certification Authority may use the following signature algorithm:

- sha256WithRSAEncryption OID = {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

7.1.4. Name formats

The Certification Authority will complete the name fields with the information established in the corresponding certificate profile, published on the website.

7.1.5. Name restrictions

No stipulation required.

7.1.6. Certificate policy object identifier

The Certification Authority will complete the certificate policy extension with object identifiers established in the corresponding section of this policy, when they adhere directly.

In case of creating its own policy, in the cases permitted by this certificates policy, an object identifier specifically defined to this effect will be included.

7.1.7. Policy restrictions extension use

No stipulation required.

7.1.8. Syntax and semantics of the policy qualifiers

The Certification Authority will include a policy qualifier in the certificates, with the following elements:

- CPS Pointer

- Explicit Text

CPS Pointer must include a URI reference in the verification general conditions for certificates issued by the Certification Authority.

Explicit Text must contain a concise declaration concerning certificate.

7.1.9. Semantics of process of certificate policy critical extension

No stipulation required.

7.1.10. Technical specifications for all Certification Authorities

The Certification Authorities must respect the technological uses generally accepted and adapt to good practices and to the most advanced technical requirements.

Additionally, renewal of Certification Authorities immediately after this CPS version will respect the following technical specifications:

- The used algorithm must be renewed when a risk of de-encryption has been advised by the community. Certification Authorities will incorporate SHA-256 after this CPS issuance.
- Certificate serial numbers will always be integers and positive.
- UTF-8 coding
- “authorityKeyIdentifier” extension will be simplified
- OIDs generated by Intermediate Certification Authorities will be restricted.

7.2. Certificate revocation list profile

Access to information related to the certificate revocation list is published on the Consorci AOC website https://www.aoc.cat/catcert/regulacio.

7.3 OCSP Profile

OCSP services comply with IETF RFC 6960.

8. Conformity audit

The Certification Authority will periodically conduct a conformity audit designed for proving compliance with security and operation requirements for being part of Cataluña certification public hierarchy.

The Certification Authority may delegate the audit execution to a third party contracted by Consorci AOC. In such cases the Certification Authority will cooperate entirely with the third party personnel assigned to conducting the investigation.

The Associated Certification Authority will periodically conduct a conformity audit designed for proving compliance, once it has started to operate, with security and operation requirements for being part of Cataluña certification public hierarchy.

The Associated Certification Authority must be prepared to pass other revisions, not periodically, that demonstrate its confidence:

- Before accepting a new Certification Authority subordinated within the hierarchy, Consorci AOC must conduct a revision of their security documents, CPS and CPs to assure that they are compliant with the security and operational requirements that form part of the Consorci AOC Certification Authorities Hierarchy.
- If at any moment there is a suspicion that the Associated Certification Authority, once in operational effect, does not comply with any of the security requirements, or if a key breach has been detected -whether suspected or proven - or any event that may present danger to security or integrity of the Associated Certification Authority, a internal audit must be conducted .

The Associated Certification Authority may delegate the execution of audits to a third party, and must cooperate entirely with the personnel assigned to conducting the investigation

8.1. Frequency of conformity audit

The Certification Authority must conduct the conformity audit annually, aside from other internal audits that may be conducted under its own criteria anytime, upon a suspicion of any security measures having been breached or key security breach.

8.2. Identification and qualification of the auditor

The Certification Authority 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 from the Certification Authority.

8.4. List of elements to be audited

The following elements are subjected to audit:

- Certification Authorities processes and related elements
- Information systems
- Protection of the process centre
- Documents

8.5. Required actions resulting from lack of conformity

Once the audit report is received, the Certification Authority discusses, either with the entity that has conducted the audit and Consorci AOC, regarding any findings and develops and executes a corrective plan to address.

If the Certification Authority, once audited, is not able to develop and/or execute the referred plan, or if the finding may indicate an immediate threat to system security or integrity, one of the following actions must be performed:

- Revoke the Certification Authority key, as described in section 4.9 of this CPS.
- End the Certification Authority service, as described in section 5.8 of this CPS.

8.6. Treatment of audit reports

Audit result reports shall be delivered to Consorci AOC, since it is the CSP, within a period of maximum 15 (fifteen) 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 the Certification Authority applies for its service provision. These rates can be consulted on the Consorci AOC website.

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 possibles to establish a certificate status access information rate.

9.1.4. Other services rates

No additional stipulation required.

9.1.5. Reimbursement policy

Consorci AOC shall not make reimbursements. For defective product cases, these shall be replaced by another in good condition.

9.2. Financial capacity

9.2.1. Civil liability insurance

Consorci AOC has a guarantee of coverage sufficient for its civil liability, under the terms provided in the electronic signature and trusted services applicable regulation. This insurance covers the activities of Consorci AOC as a TSP.

In case of incorrect or non-authorised use of certificates, Consorci AOC (or the corresponding Associated Certification Authority) will not act as a trustee towards subscribers and third parties, who shall address towards the offender of certificate usage conditions established by Consorci AOC (or the corresponding Associated Certification Authority).

9.2.2. Other assets

No stipulation required.

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

In cases of incorrect or unauthorized use of certificates, the Certification Authority shall not act as a trustee towards subscribers and third parties, who shall address towards the offender of certificate use conditions established by Consorci AOC (or the Certification Authority).

9.3. Confidentiality

9.3.1. Confidential information

The following confidential information is maintained by the Certification Authority:

a. Business information provided by its suppliers and other people with whom Consorci AOC or the Certification Authority have an obligation of confidentiality, legally or conventionally established.

b. Transactions registers, including complete registers and transaction audits registers.

c. Internal and external audit registers, created and/or maintained by the Certification Authority and its auditors.

d. Business continuity and emergency planning.

e. Security policies and plans.

f. Operational documentation such as archive, monitoring and others.

g. Any other information classified as confidential.

9.3.2. Non confidential information

The following information is not classified as confidential:

- This CPS and the CP of Consorci AOC.
- Information contained in the certificates.
- Any information whose publicity is imposed by regulation.
- Any other information identified as public.

9.3.3. Responsibility for protection of confidential information

The Certification Authority is responsible for establishing the appropriate protection measures for confidential information.

These measures include confidential information appropriate clauses which all persons involved in the corresponding certification processes will be submitted.

9.4. Personal data protection

9.4.1. Personal Data Protection Policy

Consorci AOC develops a personal data protection policy according to the applicable data protection regulation.

In particular, and in compliance with the obligations imposed by the Regulation (EU) Nº 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and the free circulation of these data and by which Directive 95/46 / CE -General data protection regulation is repealed, and Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter, LOPDGDD), has a register of personal data processing activities, in which the following files are collected:

The structure of personal data processing is:

1. Certificate subscribers: https://www.seu-e.cat/documents/31307/0/RAT_SubscriptorsColectiusCertificats/f70ee619-882e-40ab-b926-4e300d160da3

2. Certified physical persons: https://www.seu-e.cat/documents/31307/0/RAT+-+Persones+f%C3%ADsiques+certificades/a943e588-6744-43e5-8ae4-1e87d570591f

Consorci AOC develops the procedures indicated in this document, then implements them within its services provision, where in compliance with the requirements established by the certificates policy, the requirements and obligations related to personal data obtention and management are described.

Consorci AOC establishes technical and organisational security measures in order comply with security requirements applicable to files and automated treatments.

9.4.2. Personal data not available for third parties

In accordance with the provisions of Article 4 GDPR, personal information is considered any information related to identified or identifiable natural persons.

Personal information that is not to be included in the certificates and in the indicated mechanism for checking the status of the certificates, is considered personal information of a private nature.

The following data are considered in any case as private information:

- Certificate requests, either approved or denied, and any other personal information obtained for certificates issuance and maintenance.
- Private keys generated and/or stored by the Certification Authority.
- Any other personal data that is not to be searched, stored or accessed by third parties.

9.4.3. Personal data available for third parties

This section refers to personal information included in the certificates and the referred certificates status check mechanisms, according to section 3.1 of this document.

The referred information, provided by the certification request in accordance with terms of the applicable legislation, is included in the certificates and the certificates status check mechanism.

This personal data must be available by third parties due to legal imperative ("public data").

The following information is considered not confidential:

a. Issued certificates or those under issuance process.
b. The subscriber connection to a certificate issued by the Certification Authority.
c. Full name of the certificate subscriber, as well as any other circumstances or personal data of the holder, if they are significant for the certificate purpose, according to this document.
d. Email address of the certificate subscriber.
e. Economic uses and limitations described in the certificate.
f. Certificate validity period, issuance date and expiration date.
g. Certificate serial number.
h. Different certificate status and the start date of each, in particular: pending issuance and/or delivery, valid, revoked, suspended or expired and the reason for the change state.
i. CRLs and all information regarding revocation status.
j. Information contained in the public part of the Certification Authority Register.

9.4.4. Responsibility corresponding to personal data protection

Confidential information is protected, in accordance with the GDPR, from its loss, destruction, damage, falsification and illegal or unauthorized processing.

In the event of any breach of security or loss of integrity that has a significant impact on the trust service provided or the corresponding personal data, the Consorci AOC will notify the national supervisor responsible for information security or the Protection of Information Authority. corresponding data, in a maximum period of 24h after to have the knowledge of the facts, according to the article 19.2 eIDAS Regulation.

9.4.5. Incident management related to personal data

Consorci AOC includes in this document the notification, management and response procedures in relation to incidents related to personal data.

This notification procedure is directly initiated when the system administrator of the Certification Authority, within their facilities, communicates by telephone with the Certification Authority Responsible, describing type of incidents and observed effects.

During incident management if software or system configuration modifications are required, or security copies must be restored or other similar interventions, the administrator will wait

until receipt of the corresponding digitally signed request (by email) that the Certification Authority Responsible or the technical responsible of the affected project will send (in this case, adding in copy the Certification Authority Responsible).

Once the necessary actions are performed and normal system functions have been resumed, the system administrator sends to the Certification Authority Responsible a descriptive report by email, which in cases of incidents related to files containing personal data, will only contain the form duly completed.

The Certification Authority Responsible keeps a copy of the forms corresponding to incidents registered within the last 12 months related to files containing personal data. Forms are stored in a dedicated directory within the server that users of the Certification Authority share, protected as so only to be accessed by authorised personnel; in this way it is guaranteed that content security copies are made.

The Incident Register form contains the following data:

- Which resource the incident has been recorded against
- Code and description
- Date and time
- Type of incident
- Effects
- Who has reported and who receives the incident
- The response
- Procedures to be conducted
- The person who will conduct them
- Recovery procedure
- The person with authorisation to make the recovery.
- Restored data

9.4.6. Personal data processing

Consorci AOC, for its service provision, is required to collect and store certain information that implies personal data treatment.

Consorci AOC informs the key holders regarding their personal data being obtained.

The personal information collected from registered users is stored in the database owned by the AOC Consortium that assumes technical, organizational and security measures that guarantee the confidentiality and integrity of the information in accordance with the provisions of the RGPD, and Other applicable legislation.

The user will be liable, in any case, for the veracity of the data provided, consortium AOC reserving the right to exclude from the registered services any user who has provided false data, without prejudice to the other legal actions.

Any registered user can at any time exercise the right of access, rectification or deletion, opposition, limitation to treatment and portability, by request to the AOC Consortium C / Tangier 98, 22 @ - 08018 Barcelona or by electronic form (https://www.seu-

e.cat/web/consorciaoc/govern-obert-i-transparencia/serveis-i-tramits/tramits/tramits-associats-a-la-lopd-193)

However, if the user considers that his right to the protection of personal data has been violated, he can claim before the Catalan Data Protection Authority.

9.4.7. Personal data communication

Consorci AOC only communicates personal data to third parties in legally established cases.

In particular, Consorci AOC is obliged to reveal the identity of the signatories when judicial bodies require so in the exercising of its functions and other assumptions described in the personal data protection applicable regulation.

Consorci AOC complies to all legal prescriptions in conformance with the GDPR and LOPDGDD.

Exceptionally, in the case of activity cease by the Certification Authority, Consorci AOC will cede the personal data for the assumption of service provision transfer.

9.5. Property rights

9.5.1. Certificates and revocation information property

Consorci AOC in the only entity that retains the property rights to the certificates they issue.

Consorci AOC concedes non exclusive license to reproduce, distribute, verify and use certificates, without any cost, regarding digital signatures and/or encryption systems within the application scope of this CPS, according to the corresponding to the binding instrument between Consorci AOC and the party that reproduces and/or distributes the certificate.

The referred regulations figure in the legal instruments between Consorci AOC and subscribers and verifiers.

Additionally, certificates issued by Consorci AOC contain a legal advice related to certificate property. This regulation is also applied in the use of certificates revocation information.

9.5.2. Certification Practice Statement and Certification Policy property

Consorci AOC is the only entity that retains property rights of the certification policies of the Catalonia certification public hierarchy.

Consorci AOC is the owner of this CPS. The Consorci AOC does not charge a fee for access to this CPS or to the different PCs. Any use made for purposes other than simply viewing the documents, such as reproduction, redistribution, modification or creation of a derivative thereof, will be subject to a license agreement with the entity that owns the copyright of the document.

9.5.3. Property of information related to names

The subscriber (key holder, as the case may be) preserves rights related to brand, product or commercial name contained in the certificate.

The subscriber (key holder, as the case may be) is the owner of the certificate distinguished name, formed by the information specified in section 3.1. of this CPS.

9.5.4. Keys property

Key pairs become the property of the certificate subscribers.

When a key is divided in parts, all parts of the key become the property of the key holder.

9.6. Obligations and civil liability

9.6.1. The Certification Authority

9.6.1.1. Obligations and other commitments

The Certification Authority has to comply with the following:

- Determines the subscribers and verifiers community of the Certification Authority.
- Approves certification policies and in given cases, certificate specified policies.
- Approves contractual and regulatory documentation related to certification services in the users community of the Certification Authority, according to the procedure of this CPS.
- Informs Consorci AOC promptly regarding all information related to changes to be performed, service incidents, reclaims, denounces and service inspections.
- Guarantees, within their responsibility, compliance with all requirements established in this CPS.
- Be the singular entity responsible for compliance with the procedures described in this CPS, even where operations are partially or fully subcontracted externally.
- Provide certificates services according to this CPS, where the contents of the applicable legislation are described in section 9.15.
- In accordance with the applicable law, prior to certificate issuance and delivery, the Certification Authority informs of the aspects described in the applicable legislation and others as follows:
    - Indication of applicable policy, indicating that certificates are not issued to the public and the need of usage of a qualified device for signature creation.
    - How the patrimonial responsibility of the Certification Authority is guaranteed.
    - The Certification Authority agrees the certification policy, the Certification Services Provider certification and the certification of the used electronic signature products.

  This requirement is accomplished via an applicable “PKI Disclosure Statement (PDS)” electronically transmitted using a long-term communication method and comprehensible language.
- The Certification Authority obliges the subscribers, key holders and verifiers, via appropriate legal instruments transmitted electronically with written and comprehensible language, to consider the following contents:
    - Prescriptions to comply with this CPS.
    - Indication of applicable policy, indicating that certificates are not issued to the public and the need of usage of a qualified device for signature creation.
    - Manifestation that the contained information in the certificate is correct, except where contrary notification from the subscriber is made.
    - Consent for certificate publication in the directory and access to same by third parties.
    - Consent for the storage of information used for the subscriber and key holder register, the provision of the signature creation qualified device and the cession of the referred information to third parties, in case of operations end of the Certificate Authority without revocation of valid certificates.
    - Certificate limitations of use, including the established limitations in section 4.5 of this CPS.

- Information about how to validate a certificate, including the requirement of checking the certificate status and conditions in which the certificate may reasonably be trusted (this is applicable when the subscriber acts as verifier).
- Applicable responsibility limitations, including uses for which the Certification Authority accepts or excludes its responsibility.
- Procedures applicable to disputes resolution. .
- Applicable law and competent jurisdiction.

The Certification Authority identifies the key holder according to the legislation applicable in this CPS. Specifically, the Certification Authority verifies autonomously the identity and other personal circumstances of the certificate applicants.

9.6.1.2. Guarantees offered

9.6.1.2.1. Guarantees offered to subscribers

The Certification Authority guarantees the subscribers:

a. Compliance with their legal obligations as CSP, according to applicable legislation.
b. There are no errors in the information contained in the certificates, known or performed by the Certification Authority, or due to lack of diligence in the management of the certificate request or creation.
c. Certificates comply all material requirements established in the CPS.
d. Revocation services and directory use comply with all material requirements established in the CPS.
e. In case of the private keys being generated, confidentiality is maintained during the process.
f. The responsibility of the Certification Authority with the established limitations.

9.6.1.2.2. Guarantees offered to the verifiers

The Certification Authority guarantees the verifiers>

a. Compliance with their legal obligations as a TSP, according to applicable legislation.
b. The information contained or incorporated by reference in the certificate is correct, except when the opposite is indicated.
c. In cases of certificates published in the directory, the certificate has been issued to identified subscriber and the certificate has been accepted according to section 4.4 of this CPS.
d. In the certificate request approval and issuance, that all material requirements established in this CPS have been complied with.
e. The speed and security in the services provision, in particular revocation and directory services.

f. Certificates comply all material requirements established in this CPS.

g. In case of the private keys being generated, confidentiality is maintained during the process.

h. Revocation services and directory use comply all material requirements established in this CPS.

The responsibility of the Certification Authority with the established limitations .

9.6.2. Register Authorities

9.6.2.1. Obligations and other commitments

9.6.2.1.1. Obligations of Internal Register Authorities

The Internal Register Authority will be obliged to:

a. Name as (technical) register authority operators two or more employees (depending on the EC, in general four or more) and communicate these persons data to Consori AOC in order to issue the corresponding operator certificates. When an operator leaves their role, the Internal Register Authority has to immediately request this operator certificate revocation to the Associated Certification Authority.

b. Validate and approve certificate requests and generate certificates for the hey holders, according to technical procedures and instruments established by the Associated Certification Authority, in accordance with the CPS and Associated Certification Authority operational documentation.

c. If the Register Authority does not have updated information related to the key holder, verify the identity in person or in accordance with the provisions of the applicable law, described in section 9.15 of this CPS, and register a justifying of full name accreditation, date and place of birth, National Id Document and/or any other information that may be used to differentiate between two persons within the Internal Register Authority scope.

d. Verify, when necessary, any specific attribute of the key holder and register an information accreditation justifyin.

e. Perform or process certificate suspension, enablement, revocation and renewal requests, according to technical procedures and instruments established by the Associated Certification Authority, in accordance with the CPS and the Associated Certification Authority operational documentation.

f. Store registers related to certificate contained information, both in paper or electronic, with the appropriate security, authenticity, integrity and preservation measures, for a period of 15 (fifteen) years from the expiration of the certificate or the end of the service provided and, in any case, during the period established by current legislation. These registers must be available for the Associated Certification Authority.

g. Store certificate delivery form for a period of 15 (fifteen) years. These registers must be available for the Associated Certification Authority.

9.6.2.1.2. Virtual Register Authority

The Virtual Register Authority is obliged to:

a. Provide necessary documental justification for user register and certificate issuance by the Associated Certification Authority or the Collaborator Register Authority.

b. The documental justification must be performed by body unit of the Virtual Register Authority (indicated to Consorci AOC) legally entitled to attest the data to be certified.

9.6.2.1.3. Collaborator Register Authority

The Certification Authority will be able to delegate some functions to the Collaborator Register Authority, which will be obliged to comply in the same conditions than the Certification Authority.

The Collaborator Register Authorities will support the subscribers of certificates issue to the institutions with Virtual Register Authority, and all the subscribers of other certificates.

The Collaborator Register Authority will act on its own behalf, without prejudice to the responsibility of the Associated Certification Authority.

The Collaborator Register Authority is obliged to register and approve (if correct) the certificate data. Using this register all required checks related to subscriber identity, personal and complementary data will be done, and if needed, to the key holder.

This verifications must include the documental justification provided by the applicant, and in case that the Collaborator Register Authority considers, any other relevant document or information, facilitated by the subscriber, key holder or third parties.

If the Collaborator Register Authority detects errors in the data that must be included in the certificate or in the documents that justify this data, they will be obliged to change what they consider necessary before the issuance, or to stop the issuance process and manage the corresponding incident with the subscriber.

In the case that the Collaborator Register Authority corrects data without the corresponding previous incident management with the subscriber, they will be obliged to notify the subscriber of the data that is eventually certified at the time of the delivery.

The Collaborator Register Authority reserves the right to not approve the certificate issuance request when the documental justification provided by the applicant is not sufficient for correct identification and/or authentication of the subscriber, or if necessary, the key holder.

9.6.2.2. Guarantees offered to subscriber and verifier

9.6.2.2.1. Consorci AOC guarantee for digital certificate services

Consorci AOC guarantees that the Certification Authority private key used to issue certificates has not been compromised, except of Consorci AOC communicating the contrary, according to this CPS.

Consorci AOC guarantees that:

a. Electronic signature certificates contain all the information required by Law 6/2020, of November 11, eIDAS Regulation (UE) nº 910/2014 and other applicable regulations, which are described in section 9.15.

b. The process has not originated or introduced false or wrong statements in any certificate information, and has included the necessary information provided by the subscriber and validated by Consorci AOC or the Collaborator Register Authority, at the time of certificate issuance.

c. All certificates comply with the formal and content requirements of the CP and its corresponding Certification Profile.

d. Remaining associated to operations, security and archive procedures described in this CPS.

9.6.2.2.2. Guarantee exclusion

Consorci AOC does not guarantee any software used by the subscriber or any other person to generate, verify or not use any digital signature or certificate issued by Consorci AOC in a different way, except for cases where there is a statement written by Consorci AOC to the contrary.

9.6.3. Subscribers

9.6.3.1. Obligations and other commitments

9.6.3.1.1. Requirements for all type of certificates

The Certification Authority obliges the subscriber to:

a. Facilitate towards the Certification Authority the appropriate and complete information according to the requirements of this CPS, specifically related to the register procedure.

b. Manifest their consent prior to a certificate issuance and delivery.

c. Comply with the obligations for subscribers established in this CPS and in the legislations described in section 9.15 in this CPS.

d. Use the certificate in accordance with the provisions of section 1.4 of this CPS.

e. Notify the Certification Authority, without unjustifiable delay, of the loss, alteration, non-authorised use, theft or compromise of their signature creation qualified device.

f. Notify (without unjustified delay) the Certification Authority and any other person who may trust in the certificate:

    a The loss, theft or potential compromise of private keys.

    b The loss of control over their private key due to activation data breach (for example, PIN code of the signature creation qualified device) or any other cause.

    c Inaccuracies or changes in the contents of the certificate that the subscriber may know.

g. Stop using the private key once the period indicated in the corresponding section is expired.

h. Transfer to the key holders their specified obligations.

i. Not to monitor, manipulate or perform reverse engineering of technical implantation of the public certification hierarchy of Catalonia without previous written permission.

j. Not to intentionally compromise the public certification hierarchy of Catalonia security.

9.6.3.1.2. Specific requirement for qualified electronic signature certificates

The Associated Certification Authority will obliged the subscriber to:

a. Use the key pair exclusively for electronic signatures and according to any other notified limitation.

b. Be diligent in the custody of their private key and signature creation qualified device, with the purpose of avoiding non-authorised uses.

c. If the subscriber generates its own keys, they are obliged to:

    1. Generate is subscriber keys using an algorithm recognised as suitable for qualified electronic signature.

    2. Create the keys within the signature creation qualified device.

    3. Use key lengths and algorithms recognised as suitable for qualified electronic signature.

e. Notify the Certification Authority, without unjustifiable delay, the loss, alteration, non-authorised use, theft or compromise of their signature creation qualified device

9.6.3.2. Guarantees offered by the subscriber

The Certification Authority obliges the subscriber, via corresponding legal instrument, to guarantee that:

a. All the manifestations performed in the request are correct.

b. All the informations provided by the subscriber and contained in the certificate are correct.

c. A certificate is exclusively used for legal and authorised uses, according to this CPS.

d. Every digital signature created with the private key corresponding to the public key included in the certificate, is that of the subscriber, and the certificate has been accepted and it is in operation (nor expired or revoked) at the time of the signature creation.

e. The subscriber is an end-entity and not a Certification Authority and does not use the private key corresponding to the public key included in the certificate to sign any certificate (or any other certificate public key format) or CRL.

f. Non-authorised persons have never had access to the subscriber private key.

9.6.3.3. Private key protection

The Certification Authority is obliged, via the corresponding legal instrument, to guarantee that they are the unique responsible for any damage caused by the breach of duty of private key protection.

9.6.4. Verifiers

9.6.4.1. Obligations and other commitments

The Certification Authority obliges the certificate user to:

a. Accept advice regarding certificate being appropriate for its expected use.

b. Verify issued certificates validity, suspension or revocation, using status certificate information.

c. Verify all certificates within the certificate hierarchy before trusting on digital signature or any hierarchy certificates.

d. Acknowledge any certificate use limitations, whether in the certificate or in the verifier contract.

e. Acknowledge any prevention established within a contract or other instrument, regardless of the legal nature.

f. Not to monitor, manipulate or perform reverse engineering over the technical implantation of the Cataluña Certification Public Hierarchy, without previous written permission.

g. Not to intentionally compromise the Cataluña Certification Public Hierarchy security.

h. Recognise that electronic signatures performed via qualified devices of electronic signature are electronic signatures equivalent to handwritten signatures, according to article 25.2 of Regulation (EU) 910/2014.

i. Verify the validity of the certificates in the moment to perform any operation based on them.

   In this manner, the third that trust, will verify that the qualified certificate checking the trusted list in the European Union (TLS). The regulation ETSI TS 119 615 provide orientation about how to validate a digital certification with the trusted lists in the EU, with the purpose to determine if it can be considered as a qualified certificate.

9.6.4.2. Guarantees offered by the verifier

The Certification Authority obliges the verifier, via the corresponding legal instrument, to manifest that:

a. It has sufficient information to make a decision informed to trust or not to trust in the certificate.

b. It is the unique responsible for trusting or not trusting in the information contained in the certificate.

c. Will be the unique responsible for its obligations as verifier.

9.6.5. Consorci AOC

9.6.5.1. Obligations and commitments

Consorci AOC is obliged to operate the Certification Authorities under its responsibility, including the Root Certification Authority of the Cataluña Certification Public Hierarchy, in a diligent way, in accordance with policies, practices and regulations of the the referred hierarchy.

9.6.5.2. Guarantees offered to subscriber

Consorci AOC guarantees that the private key of the Certification Authorities under its responsibility has not been compromised, unless indicated via Consorci AOC directory.

Consorci AOC guarantees that:

a. Certificates contain all the information required by the applicable legislation, described in section 9.15 of this CPS, and that they have not or introduced false or wrong statements in any certificate information, and have included the necessary information provided by Certification Authority and validated by Consorci AOC or the Register Authority, at the time of certificate issuance

b. All issued certificates comply with the formal and contents requirements.

Consorci AOC is associated to operational and security procedures described in this CPS.

9.6.5.3. Guarantees offered to the verifiers

The responsibility of Consorci AOC, that derives from an indirect relationship, is the responsibility provided in the applicable legislation, described in section 9.15 of this CPS.

9.6.5.4. Guarantees exclusion

Consorci AOC does not guarantee any software used by the subscriber or any other person to generate, verify or not use any digital signature or certificate issued by Consorci AOC in a different way, except for cases where there is a statement written by Consorci AOC to the contrary.

9.6.6. Directory

9.6.6.1. Obligations and commitments

The Certification Authority may delegate some functions to the directory, which in this case is obliged to its compliance under the same conditions.

9.6.6.2. Guarantees

The Certification Authority establishes in this CPS the civil liability of the directory when operated by a third party.

9.7. Guarantee disclaimer

9.7.1. Rejection of Certification Authority guarantees

The Certification Authority may reject all service guarantees not linked to established obligations in the applicable legislation, as described in section 9.15 of this CPS, 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. Certification Authority limitations of responsibility

The Certification Authority limits its responsibility by restricting the certificate issuance and management service, and where appropriate, the subscriber key pair and cryptographic deposits (of signature and signature verification as well as encoding and decoding) provided by them.

The Certification Authority may limit its responsibility via including use limits and value limits for transactions that the certificate may be used for

9.8.2. Fortuitous event and force majeure

The Certification Authority includes clauses to limit its responsibility in fortuitous events and force majeure cases, via legal instruments with which the Certification Authority associates subscribers and verifiers.

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 and end of term

The Certification Authority establishes, within its legal instruments with subscribers and verifiers, a clause that determines the legal relation validity period, by which the Certification Authority provides certificates to the subscriber.

9.10.2. Survival

The Certification Authority establishes, within its legal instruments with subscribers and verifiers, survival clauses, establishing that certain obligations remain in force after the termination of the legal relationship regulating the service between the parties

To this effect, the Certification Authority ensures that requirements contained in Obligations, Civil Liability, Conformity Audit and Confidentiality sections, will continue in force after the end of the certification policy and the legal instruments that associate the Certification Authority with subscribers and verifiers.

Consorci AOC will determine a Business Termination Plan that will establish the obligations that Consorci AOC assumes in case of activity cease, addressed to maintain in force the issued certificates until their expirations and the use and custody of all information generated by Consorci AOC in its activity as Certification Services Provider, for example, secure copies, logs and all types of documents, regardless their support or storage. To this effect, Consorci AOC assures that a secure copy is generated periodically, as a complementary provision of the ordinary activity and of the assurance of the business continuity.

9.11. Notifications

The Certification Authority establishes, within its legal instruments associated to subscribers and verifiers, notification clauses, by which the procedure for the parties notifying facts to each other is established.

9.12. Modifications

9.12.1. Modification procedures

Consorti AOC may modify, unilaterally, the regulatory documentation of the service, as long as is appropriate following this procedure:

- Modification must be justified technically, legally and commercially.
- A modification control is established in order to guarantee, in all cases, that the resulting specifications comply with the requirements to be accomplished and that originated the change.
- Implications that the specifications have on the user are established, and the necessity of notifying the referred modifications to the user is planned.

- Changes must be approved by Consorci AOC.

9.12.2. Term and mechanisms for notifications

Modifications to this CPS shall be notified to Consorci AOC for their approval.

9.13. Conflicts resolution

9.13.1. Conflicts extrajudicial resolution

The Certification Authority establishes, within its legal instruments with subscriber and verifiers, the procedures for mediation and resolution of applicable conflicts, considering the Certification Authority as Public Administration.

Discrepancy situations that derive from the use of certificates issued by the Certification Authority, are resolved by applying the same competence criteria than in cases of hand-written signed documents.

9.13.2. Competent jurisdiction

The Certification Authority establishes, within its legal instruments associated to subscribers and verifiers, a competent jurisdiction clause indicating that the international legal competency corresponds to the spanish judges.

The territorial and functional competency is determined by the applicable international private law regulations and procedural law regulations

Applicable administrative legislation is also considered.

9.14. Applicable law

The Certification Authority establishes, within its legal instruments with subscribers and verifiers, that the law applicable to services provision, including CPS and the CPs, is the following:

- Law 39/2015, of October 1, on the Common Administrative Procedure of Public Administrations.
- Law 40/2015, of October 1, on the Legal Regime of the Public Sector.
- Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, regarding the protection of natural persons with regard to the processing of personal data and the free circulation of these data and by which repeals Directive 95/46 / EC (GDPR)
- Organic Law 3/2018, of December 5, Protection of Personal Data and guarantee of digital rights

- Directive (EU) 2015/2366 of the European Parliament and of the Council of November 25, 2015 on payment services in the internal market and amending Directives 2002/65 / EC, 2009/110 / EC and 2013/36 / EU and Regulation (EU) No. 1093/2010 and Directive 2007/64 / CE is repealed.
- Implementing Regulation (EU) 2015/1502 of the Commission of September 8, 2015 on the setting of specifications and minimum technical procedures for the security levels of electronic identification means in accordance with the provisions of article 8, paragraph 3, of Regulation (EU) No. 910/2014 of the European Parliament and of the Council, regarding electronic identification and trust services for electronic transactions in the internal market.
- Implementing Decision (EU) 2016/650 of the Commission, of April 25, 2016, which establishes the rules for the evaluation of the security of qualified devices for the creation of signatures and stamps in accordance with article 30, section 3, and Article 39 (2) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council, on electronic identification and trust services for electronic transactions in the internal market.
- Commission Delegated Regulation (EU) 2018/389 of November 27, 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for the reinforced authentication of clients and a common and secure open communication standard.
- Latest version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published at http://www.cabforum.org by the CA / Browser Forum. In the event of any inconsistency between this Certification Practice Statement and the aforementioned requirements, those requirements will prevail.
- Guidelines For The Issuance And Management Of Extended Validation Certificates, published at http://www.cabforum.org by the CA / Browser Forum. In the event of any inconsistency between this document and those Guidelines, those Guidelines prevail over this document.
- Real Decreto 311/2022, the 3rd of May, which regulates *Esquema Nacional de Seguridad*
- The Normative framework for Information Security of the Cybersecurity Agency of Catalonia which determines the strategic, politics, standards lines and own security guides from the Generalitat de Catalunya, with supplementary character in the absence of an own one.
- Security Policy from AOC.

In case of inconsistency between the applicable national law and the requirements of the CA / Browser Forum, this CPS will be adjusted to align with the requirements of the national law, but the Consorci AOC will notify the CA / Browser Forum of such adjustment.

9.15. Conformity with applicable law

Consorci AOC will be responsible for damages caused to users or third parties by its services according to the legislation in force and this CPS.

9.16. Diverse clauses

9.16.1. Entire agreement

The Certification Authority establishes, within its legal instruments associated to subscriber and verifiers, entire agreement clauses, by which understands that the legal instrument that regulates the service contains all the good intentions and all agreements between parties.

9.16.2. Surrogacy

Rights and duties associated to Certification Authority condition may not be transferred to any third parties, and no third entity may surrogate in the legal position of a Certification Authority.

In case cession or surrogacy, the referred Certification Authority will end.

Rights and duties associated to Virtual Certification Authority condition may be transferred or subrogated, but these incidents must be notified to Consorci AOC.

9.16.3. Divisibility

The Certification Authority establishes divisibility clauses, within its instruments associated with subscribers and verifiers, by which an invalid clause does not affect the rest of the contract.

Given the case that, as cause of articles 7 and 8 of Law 7/1998, of April 13, regarding hiring general conditions, any of the indicated clauses will be considered as non incorporated or invalid. The referred non incorporation or nullity will not determine the total inefficiency of the contract, if the contract could persist without the referred clauses.

9.16.4. Applications

No stipulation required.

9.16.5. Other clauses

No stipulation required.