Consorci
Administració Oberta
de Catalunya

Profile description of Consorci AOC Certificates

Generalitat de Catalunya

LOCALRET

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

Record of versions

Version	Summary of amendments	Date
5.0	EIDAS adaptation	9/05/2018
6.0	Consolidation in a single document of the profiles document issued by EC-SECTORPUBLIC and EC-CIUTADANIA	26/07/2018
6.1	• Annual review of the documentation, post audit eIDAS. • "*4.4. Profile of the Secure Server Certificates (Dispositiu SSL)*": Removed multidomain or wildcard option.	24/07/2019
6.2	• "2.6: Profile of public employee signing certificates with a high level pseudonym". Inclusion of EKU • "2.8. Profile of High Level Public Employee Signature Certificates". Inclusion of EKU	31/3/2020
6.3	• Inclusion of mid-level and high-level public worker authentication and signature certificates	03/08/2020
6.4	• Document review	27/01/2021
6.5	• Document review	20/07/2021
6.6	• "3.1.1 Certificates": Change in the description C = Country of issue of the subscriber identification document	31/03/2022

Table of contents

1. Introduction

This document of certificate profiles description has the objective of outlining the content of certificates issued by Consorci AOC, according to requirements established by the Ministry competent in electronic trust services; in other words, it specifies the configuration (mainly National Document, Name and Description fields) and the extension (Extension, Critic -yes/no, and Values) of personal certificates for public server, citizen certificates and devices and infrastructure certificates, each one of them with their own Certification Policy (accessible from URL https://www.aoc.cat/catcert/regulacio). It also refers to Common Name (CN) field composition in those cases when the certificates include this.

Certificate issuance has been executed according to Regulation (EU) 910/2014 of European Parliament and Council of 23th July 2014, regarding electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1993/93/CE (eIDAS from here on). It has also taken as reference the document "Perfiles de certificados electrónicos", 1st electronic edition from april 2016, which is available in Portal de Administración Electrónica (PAe): http://administracionelectronica.gob.es/

2. Description of the profiles of personal certificates of the public sector

2.1. Profile of the high-level authentication certificate for public employee (T-CAT authenticació)

2.1.1. Certificate

Field of the DN	Name	Descripción
O, Organization	Organization	Denomination (“official” name) of the Administration, organism or public entity subscribing the certificate, to which the employee is bound.
OU, Organization Unit	Organization Unit	“Empleat públic de nivell alt d'autenticació”
Title (optional)	Title	Shall include the title that links the natural person to the administration, organism or public entity subscribing the certificate.
SN, Serial Number	NIF	Signatory Identification document number, with the semantic proposed by the standard ETSI EN319412-1[1]
Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, …) + "-DNI" + NIF of the public employee.
Given name	Name	Name and two surnames according to the Identification document (DNI, passport,...)
CN, Common Name	Name, surname and NIF	Name and two surnames according to the Identification document (DNI/Passport)+ "-DNI" + NIF of the public employee + "(AUT)”
C, Country	Country	C = “ES”
Organization Identifier		According to the technical standard ETSI EN 319 412-1 (VATES + NIF de la entidad)

[1] Serial Number = e. g: IDCES-00000000G. 3 characters to denote the document type (IDC= national identification number, PAS=Passport, ...) + 2 characters to denote the country (ES) + Identification number (Printable String)) Size [RFC 5280] 64

2.1.2. Extensions

Extension	Critic	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question >
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Yes	Digital Signature Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associated with the DPC> 1: 1.3.6.1.4.1.15096.1.3.2.7.1.2 <URI of the DPC> <User Notice> " Certificat electrònic d'empleat públic de nivell alt d'autenticació . Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID of the certification policy of high-level certificate for public servant>2.16.724.1.3.5.7.1 <OID of the certification policy ETSI: NCP+> 0.4.0.2042.1.2
X509v3 Subject Alternative Name	-	(optional for SMIME) rfc822Name: contact mail (optional) otherName-userPrincipalName (UPN):Windows domain user of the key holder directoryName: OID: 2.16.724.1.3.5.7.1.1 = "Certificat electrònic d'empleat públic de nivell alt d'autenticació" OID: 2.16.724.1.3.5.7.1.2 = <O of DN> OID: 2.16.724.1.3.5.7.1.3 = <CIF of subscriber entity> OID: 2.16.724.1.3.5.7.1.4 = <serialNumber of DN> OID: 2.16.724.1.3.5.7.1.6 = <Given name> OID: 2.16.724.1.3.5.7.1.7 = <First surname of the public servant>

		OID: 2.16.724.1.3.5.7.1.8 = <Second surname of the public servant>

2.2. Profile of the mid-level qualified certificates of authentication and signature for public employee(T-CATP)

2.2.1. Certificate

Field of the DN	Name	Description
O, Organization	Organization	Denomination (“official” name) of the Administration, organism or public entity subscribing the certificate, to which the employee is bound.
OU, Organization Unit	Organization Unit	“Empleat públic de nivell mig”
Title (optional)	Title	Shall include the title that links the natural person to the administration, organism or public entity subscribing the certificate.
SN, Serial Number	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN319412-1[2]
Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, …) + "-DNI" + NIF of the public employee.
Given name	Name	Name, according to the Identification Document (DNI, Passport, …)
CN, Common Name	Name, Surname and NIF	Name and two surnames according to the Identification document (DNI/Passport)+ "-DNI" + NIF of the public employee + "(TCAT")"
C, Country	Country	C = “ES”
Organization Identifier		According to the standard ETSI EN 319 412-1 (VATES + entity NIF)

[2] Serial Number = e. g: IDCES-00000000G. 3 characters to denote the document type (IDC= national identification number, PAS=Passport, ...) + 2 characters to denote the country (ES) + Identification number (Printable String)) Size [RFC 5280] 64

2.2.2. Extensions

Extension	Critic	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Subject Key Identifier	-	<certificate public key id, obtained from its hash>
X509v3 Authority Key Identifier	-	<certificate public key of the CA, obtained from its hash>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URI of the certificate of the sender EC>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Yes	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage		Email protection Client Authentication
X509v3 Certificate Policies	-	<OID of the DPC> 1.3.6.1.4.1.15096.1.3.2.7.3.1 <URI of the DPC> <User Notice> “Certificat electrònic d'empleat públicd’e empleattreballador públic de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A” <OID that states the mid-level public employee electronic certificate > 2.16.724.1.3.5.7.2 <OID of the certification policy ETSI: QCP-n> 0.4.0.194112.1.0
Qualified Certificate Statements		Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1

X509v3 Subject Alternative Name	-	rfc822Name: contact mail (Optional) directoryName: OID: 2.16.724.1.3.5.7.2.1 = = “Certificat electrònic d’empleat públic de nivell mig” OID: 2.16.724.1.3.5.7.2.2 = <O of DN> OID: 2.16.724.1.3.5.7.2.3 = <CIF of the subscriber entity> OID: 2.16.724.1.3.5.7.2.4 = <serialNumber of DN> OID: 2.16.724.1.3.5.7.2.6 = <Given name> OID: 2.16.724.1.3.5.7.2.7 = <First surname of the public employee > OID: 2.16.724.1.3.5.7.2.8 = <Second surname of the public employee> OID: 2.16.724.1.3.5.7.2.9 = <mail of the public employee>

2.3. Profile of the authentication and signature certificate for mid-level associated persons (T-CATP persona vinculada)

2.3.1. Certificate

DN Field	Name	Description
O, Organization	Organization	Denomination (“official” name) of the Administration, organism or public entity subscribing the certificate, to which the employee is bound.
OU, Organization Unit	Organization Unit	“Persona vinculada de nivell mig”
Title (optional)	Title	Shall include the title that links the natural person to the administration, organism or public entity subscribing the certificate.
SN, Serial Number	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN 319 412-1[3]
Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, …) + "-DNI" + NIF of the public employee.
Given name	Name	Name, according to the Identification Document (DNI, Passport, …)
CN, Common Name	Name, Surname and NIF	Name and two surnames according to the Identification document (DNI/Passport)+ "-DNI" + NIF of the public employee + "(TCAT")"
C, Country	Country	C = “ES”
Organization Identifier		According to the standard ETSI EN 319 412-1 (VATES + entity NIF)

[3] Serial Number = e. g: IDCES-00000000G. 3 characters to denote the document type (IDC= national identification number, PAS=Passport, ...) + 2 characters to denote the country (ES) + Identification number (Printable String)) Size [RFC 5280] 64

2.3.2. Extensions

Extension	Critic	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Yes	Digital Signature Content Commitment Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication
X509v3 Certificate Policies	-	<OID of the DPC> 1.3.6.1.4.1.15096.1.3.2.86.1 <URI of the DPC> <User Notice> "Certificat electrònic de persona vinculada de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID of the certification policy ETSI: QCP-n> 0.4.0.194112.1.0
Qualified Certificate Statements		Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Subject Alternative Name	-	rfc822Name: (optional)contact mail (Optional)

2.4. Profile of the authentication and signature certificate for high-level associated persons (T-CATP persona vinculada)

2.4.1. Certificate

DN Field	Name	Description
O, Organization	Organization	Denomination (“official” name) of the Administration, organism or public entity subscribing the certificate, to which the employee is bound.
OU, Organization Unit	Organization Unit	“Persona vinculada de nivell alt”
Title (optional)	Title	Shall include the title that links the natural person to the administration, organism or public entity subscribing the certificate.
SN, Serial Number	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN 319 412-1[4] shall preferably apply.
Surname	Surname (natural person)	First and second surname (according the Identification Document - DNI/Passport, …) + "-DNI" + NIF of the public employee.
Given name	Name	Name, according to the Identification Document (DNI, Passport, …)
CN, Common Name	Name, Surname and NIF	Name and two surnames according to the Identification document (DNI/Passport)+ "-DNI" + NIF of the public employee + "(TCAT")"
C, Country	Country	C = “ES”
Organization Identifier		According to the standard ETSI EN 319 412-1 (VATES + entity NIF)

[4] Serial Number = e. g: IDCES-00000000G. 3 characters to denote the document type (IDC= national identification number, PAS=Passport, ...) + 2 characters to denote the country (ES) + Identification number (Printable String)) Size [RFC 5280] 64

2.4.2. Extensions

Extension	Critic	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question >
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Yes	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType 0.4.0.1862.1.6.1
X509v3 Key Usage	Yes	Digital Signature Content Commitment Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associated with the DPC> 1.3.6.1.4.1.15096.1.3.2.82.1 <URI of the DPC> User Notice: “Certificat electrònic de persona vinculada de nivell alt. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A” <OID of the certification policy ETSI: QCP-n-qscd> 0.4.0.194112.1.2
X509v3 Subject Alternative Name	-	(optional for SMIME) rfc822Name: contact mail (optional) otherName-userPrincipalName (UPN): User in Windows' domain of the key holder.

2.5. Profile of high-level authentication certificate for public employee with pseudonyms (T-CAT pseudònim autenticació)

2.5.1. Certificates

Field of the DN	Name	Description
O, Organization	Organization	Denomination (“official” name) of the Administration, organism or public entity subscribing the certificate, to which the employee is bound.
OU, Organization Unit	Organization Unit	“Empleat públic amb pseudònim de nivell alt d'autenticació”
Pseudonym	Compulsory pseudonym according to ETSI EN 319 412-2	Ej: NIP 111111111
Title (optional)	Title	Shall include the title that links the natural person to the administration, organism or public entity subscribing the certificate.
CN, Common Name	Inform with the organism pseudonym	Pseudonym + “ - “ + Title + (AUT) Ex: NIP 11111111 - SUBINSPECTOR (AUT)
C, Country	Country	C = “ES”

2.5.2. Extensions

Extension	Critic	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Subject Key Identifier	-	<id of the certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URL of the CA certificate location.>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Yes	Digital Signature Key encipherment
X509v3 Extended Key Usage		Email Protection Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associated with the DPC> 1.3.6.1.4.1.15096.1.3.2.4.1.2 <URI of the DPC> User Notice: "Certificat electrònic d'mpleat públic amb pseudònim de nivell alt d'autenticació. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID associated with high-level certificate for public servant with pseudonym> 2.16.724.1.3.5.4.1 <OID of the certification policy ETSI: NCP+> 0.4.0.2042.1.2
X509v3 Subject Alternative Name	-	(optional) otherName-userPrincipalName (UPN): User in Windows' domain of the key holder. directoryName: OID: 2.16.724.1.3.5.4.1.1 = " Certificat electrònic d'empleat públic amb pseudònim de nivell alt d'autenticació" OID: 2.16.724.1.3.5.4.1.2 = <O of DN> OID: 2.16.724.1.3.5.4.1.3 = <CIF of subscriber entity>

2.6. Profile of the signature certificates for high-level public employees with pseudonyms (T-CAT pseudònim signatura)

2.6.1. Certificate

DN Field	Name	Description
O, Organization	Organization	Denomination (“official” name) of the Administration, organism or public entity subscribing the certificate, to which the employee is bound.
OU, Organization Unit	Organization Unit	“Empleat públic amb pseudònim de nivell alt de signatura.”
Pseudonym	Compulsory pseudonym according to ETSI EN 319 412-2	Ex: NIP 111111111
Title (optional)	Title	Shall include the title that links the natural person to the administration, organism or public entity subscribing the certificate.
CN, Common Name	Inform with the organism pseudonym	Pseudonym + “ - “ + Title + (SIG) Ex: NIP 11111111 – SUBINSPECTOR (SIG)
C, Country	País	C = “ES”

2.6.2. Extensions

Extension	Critic	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question >
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URL of the CA certificate location.>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Certificate Policies	-	<OID de la DPC correspondiente> 1.3.6.1.4.1.15096.1.3.2.4.1.1 <URI of the DPC> User Notice: " Certificat qualificat de signatura d'empleat públic amb pseudònim de nivell alt. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID associated with high-level certificate for public servant with pseudonym> 2.16.724.1.3.5.4.1 <OID of the certification policy ETSI: QCP-n-qscd> 0.4.0.194112.1.2
Qualified Certificate Statements	Yes	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Yes	Email protection
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.4.1.1 = "Certificat qualificat de signatura d'empleat públic amb pseudònim de nivell alt" OID: 2.16.724.1.3.5.4.1.2 = <O of DN> OID: 2.16.724.1.3.5.4.1.3 = <CIF of subscriber entity>

2.7. Profile of the authentication and signature certificate for representatives acting before the Public Administrations (T-CAT representant)

2.7.1. Certificate

DN Field	Name	Description
O, Organization	Organization	Denomination (“official” name) of the Administration, organism or public entity subscribing the certificate, to which the employee is bound.
OU, Organization Unit	Organization Unit	“Representant davant les AAPP de nivell alt”
Title (optional)	Title	Shall include the title that links the natural person to the administration, organism or public entity subscribing the certificate.
SN, Serial Number	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN319412-1[5]
Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, …) + "-DNI" + NIF of the public employee.
Given name	Name	Name, according to the Identification Document (DNI, Passport, …)
CN, Common Name	Name, Surname and NIF	See specific schedule: Example: “12345678Z Pedro Antonio López (R: B0085974Z)”
C, Country	Country	C = “ES”
Organization Identifier		According to the technical standard ETSI EN 319 412-1 (VATES + NIF de la entidad, p.e. VATES-B0085974Z)
Description (2.5.4.13)	Representation details	Reg:XXX /Hoja:XXX /Tomo:XXX /Sección:XXX /Libro:XXX/ Folio:XXX /Fecha: dd-mm-aaaa /Inscripción:XXX Notary: Name Surname1 Surname2 /Protocol number: XXX /Fecha Otorgamiento: dd-mm-aaaa In Official Journals: Boletín: XXX /Fecha: dd-mm-aaaa /Número resolución: XXX

2.7.2. Common name

Field	Content	Example	Size(*)

[5] Serial Number = e. g: IDCES-00000000G. 3 characters to denote the document type (IDC= national identification number, PAS=Passport, ...) + 2 characters to denote the country (ES) + Identification number (Printable String)) Size [RFC 5280] 64

NIF	DNI/NIE Number	12345678Z	10
Name	According to the Identification Document	Pedro Antonio	
Surname 1	According to the Identification Document	López	
Literal	(R:		4
NIF of the represented entity.	NIF of the represented entity, as established in official registers.	Q0085974Z	9
Literal	)		2

(*) counting subsequent blank space.

2.7.3. Extensions

Extension	Critic	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question >
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Certificate Policies	-	<OID of the certification policy corresponding to the certificate> 1.3.6.1.4.1.15096.1.3.2.8.1.1 <URI of the DPC> User Notice: “Certificat electrònic de representant davant les AAPP de nivell alt. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A” <OID of the certificate of the representative of the legal person> 2.16.724.1.3.5.8 <OID of the certification policy ETSI QCP-n-qscd> 0.4.0.194112.1.2
Qualified Certificate Statements	Yes	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1

X509v3 Key Usage	Yes	Digital Signature Content Commitment Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication SmartCardLogon
X509v3 Subject Alternative Name	-	(optional for SMIME) rfc822Name: contact mail (optional) otherName-userPrincipalName (UPN): User in Windows' domain of the key holder.

2.8. Profile of high-level signature certificate for public employee (T-CAT signatura)

2.8.1. Certificate

Dn Field	Name	Description
O, Organization	Organization	Denomination (“official” name) of the Administration, organism or public entity subscribing the certificate, to which the employee is bound.
OU, Organization Unit	Organization Unit	“Empleat públic de nivell alt de signatura”
Title (optional)	Title	Shall include the title that links the natural person to the administration, organism or public entity subscribing the certificate.
SN, Serial Number	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN319412-1[6]
Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, …) + "-DNI" + NIF of the public employee.
Given name	Name	Name, according to the Identification Document (DNI, Passport, …)
CN, Common Name	Name, Surname and NIF	Name and two surnames according to the Identification document (DNI/Passport)+ "-DNI" + NIF of the public employee + "(TCAT")"
C, Country	Country	C = “ES”
Organization Identifier		According to the standard ETSI EN 319 412-1 (VATES + entity NIF)

[6] Serial Number = e. g: IDCES-00000000G. 3 characters to denote the document type (IDC= national identification number, PAS=Passport, ...) + 2 characters to denote the country (ES) + Identification number (Printable String)) Size [RFC 5280] 64

2.8.2. Extensions

Extension	Criticcs	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Yes	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Yes	Content Commitment
X509v3 Extended Key Usage	-	Email protection
X509v3 Certificate Policies	-	<OID associated with the DPC> 1.3.6.1.4.1.15096.1.3.2.7.1.1 <URI of the DPC> User Notice: " Certificat qualificat de signatura d'empleat públic de nivell alt . Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID associated with high-level certificate for public servant> 2.16.724.1.3.5.7.1 <OID of the certification policy ETSI: QCP-n-qscd> 0.4.0.194112.1.2
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.7.1.1 ="Certificat qualificat de signatura de empleat públic de nivell alt " OID: 2.16.724.1.3.5.7.1.2 = <O of DN> OID: 2.16.724.1.3.5.7.1.3 = <CIF of subscriber entity> OID: 2.16.724.1.3.5.7.1.4 = <serialNumber of DN> OID: 2.16.724.1.3.5.7.1.6 = <Given name> OID: 2.16.724.1.3.5.7.1.7 = <First surname of the public servant> OID: 2.16.724.1.3.5.7.1.8 = <Second surname of the public servant>

2.9. Profile of the Authentication Certificates and signature of public worker of medium level (T-CATP Treballador públic)

2.9.1. Certificate

Dn Field	Name	Description
O, Organization	Organization	Denomination (“official” name) of the Administration, organism or public entity subscribing the certificate, to which the worker is bound.
OU, Organization Unit	Organization Unit	“Treballador públic de nivell mig”
Title (optional)	Title	Shall include the title that links the natural person to the administration, organism or public entity subscribing the certificate.
SN, Serial Number	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN319412-1[7]
Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, …) + "-DNI" + NIF of the public worker..
Given name	Name	Name, according to the Identification Document (DNI, Passport, …)
CN, Common Name	Name, Surname and NIF	Name and two surnames according to the Identification document (DNI/Passport)+ "-DNI" + NIF of the public worker "(TCAT")"
C, Country	Country	C = “ES”
Organization Identifier		According to the standard ETSI EN 319 412-1 (VATES + entity NIF)

[7] Serial Number = e. g: IDCES-00000000G. 3 characters to denote the document type (IDC= national identification number, PAS=Passport, ...) + 2 characters to denote the country (ES) + Identification number (Printable String)) Size [RFC 5280] 64

2.9.2. Extensions

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key encipherment
X509v3 Extended Key Usage	-	Email protection Client Authentication
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.86.3 <URI de la DPC>https://www.aoc.cat/CATCert/Regulacio <User Notice> "Certificat electrònic de treballador públic de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID de la política de certificación ETSI: QCP-n> 0.4.0.194112.1.0
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Subject Alternative Name	-	rfc822Name: contact mail(Opcional)

2.10. Profile of High Level Public Worker Authentication and Signature Certificates (T-CAT Public Treballador)

2.10.1. Certificate

Dn Field	Name	Description
O, Organization	Organization	Denomination (“official” name) of the Administration, organism or public entity subscribing the certificate, to which the worker is bound.
OU, Organization Unit	Organization Unit	“Treballador públic de nivell alt”
Title (optional)	Title	Shall include the title that links the natural person to the administration, organism or public entity subscribing the certificate.
SN, Serial Number	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN319412-1[8]
Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, …) + "-DNI" + NIF of the public worker..
Given name	Name	Name, according to the Identification Document (DNI, Passport, …)
CN, Common Name	Name, Surname and NIF	Name and two surnames according to the Identification document (DNI/Passport)+ "-DNI" + NIF of the public worker "(TCAT")"
C, Country	Country	C = “ES”
Organization Identifier		According to the standard ETSI EN 319 412-1 (VATES + entity NIF)

[8] Serial Number = e. g: IDCES-00000000G. 3 characters to denote the document type (IDC= national identification number, PAS=Passport, ...) + 2 characters to denote the country (ES) + Identification number (Printable String)) Size [RFC 5280] 64

2.10.2. Extensions

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Sí	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_es Id-etsi- qcs-QcType 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.82.2 <URI de la DPC> https://www.aoc.cat/CATCert/Regulacio User Notice: “Certificat electrònic de treballador públic de nivell alt. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A” <OID de la política de certificación ETSI: QCP-n-qscd> 0.4.0.194112.1.2
X509v3 Subject Alternative Name	-	(optional for SMIME) rfc822Name: contact mail (optional) otherName-userPrincipalName (UPN):Windows domain user of the key holder

3. Description of Citizenship Certificate Profiles

3.1. Profiles of Citizenship Certificates (idCAT certificat)

3.1.1. Certificates

DN Field	Name	Description
CN, Common Name	Name	Signatory Name and Surname+ " - DNI " + identification document number. Ex: PEREZ MAS JOSE – DNI 123456789Z
serialNumber	Serial Number	Signatory identification document number, according to the semantic proposed by the standard ETSI EN 319 412-1
SN, surname	Surname	Signatory surname as in the in the used identification document.
GN, givenName	Name	Signatory name as in the in the used identification document.
C, Country	Country	"Country of issue of the subscriber identification document"

3.1.2. Certificates extension

Extension	Critic	Value
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Key Usage	Yes	Digital Signature Non Repudiation Key Encipherment
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Certificate Policies	-	<OID of the certification policy corresponding to the certificate> 1.3.6.1.4.1.15096.1.3.2.86.2 <URI of the DPC> User Notice: “idCAT Certificat. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A” <OID of the certification policy ETSI: 0.4.0.194112.1.0> (Corresponding to the EU qualified certificates policy issued to natural persons s “QCP-n”, not using a DSCF)
qcStatements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URI of the certificate of the issuer EC>

4. Description of certification for Devices and Infrastructure Profiles

4.1. Profile of Advanced Electronic Seal Certificate (Segell nivell mig)

4.1.1. Certificate

Field of the DN	Name	Description
O, Organization	Organization	Shall contain the denomination of the Administration pertaining to the relevant organism.
Organization Identifier		Organization identifier different from name according to the standard ETSI EN 319 412-1 (VATES + entity NIF)
OU, Organization Unit	Organization Unit	“Certificat de segell electrònic nivell mig”
SN, Serial Number	CIF	Public Administration, organ or public entity CIF.
Surname (Optional)	Surname (Natural Person)	First and second surname (according the Identification Document -DNI/Passport, …) + "-DNI" + NIF of the private key holder.
Given name (Optional)	Name (natural person)	Name, according to the Identification Document (DNI, NIE) of the private key holder.
CN, Common Name	Name of the application or system	e. g. “PLATAFORMA DE VALIDACIÓN DE L’AJUNTAMENT DE xxx”
C, Country	Country	C= ES.

4.1.2. Certificates extension

Extension	Critic	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Key Usage	Yes	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	Email protection TLS Web Client Authentication
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Yes	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-eseal 0.4.0.1862.1.6.2

4.1.3. Mid-level Extensions

Extension	Critic	Values
X509v3 Certificate Policies	-	<OID of the certification policy corresponding to the certificate> 1.3.6.1.4.1.15096.1.3.2.6.2 <URI of the DPC> User Notice: "Certificat de segell electrònic nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID associated with stamp certificates of mid/substantial level> 2.16.724.1.3.5.6.2 <OID "for EU qualified certificates issued to legal persons" according to ETSI EN 319 411-2: QCP-l> 0.4.0.194112.1.1
X509v3 Subject Alternative Name	-	rfc822Name: contact mail directoryName: OID: 2.16.724.1.3.5.6.2.1 = "Certificat de segell electrònic nivell mig" OID: 2.16.724.1.3.5.6.2.2 = <O of DN> OID: 2.16.724.1.3.5.6.2.3 = <serialNumber of DN> OID: 2.16.724.1.3.5.6.2.4 = <NIF/NIE del keeper> OID: 2.16.724.1.3.5.6.2.5 = <CN of the DN> OID: 2.16.724.1.3.5.6.2.6 = <Given name> OID: 2.16.724.1.3.5.6.2.7 = < First surname of thel keeper> (1) OID: 2.16.724.1.3.5.6.2.8 = <Second surname of the keeper> (2) OID: 2.16.724.1.3.5.6.2.9 = <Email of the keeper>

1. According to the identification document (DNI, NIE)
2. According to the identification document (DNI, NIE)

4.2. Profile of the Application Certificates (Dispositiu aplicació)

4.2.1. Certificate

DN Field	Name	Description
O, Organization	Organizations	Shall contain the denomination of the Administration pertaining to the relevant organism.
Organization Identifier		Organization identifier different from name according to the standard ETSI EN 319 412-1 (VATES + entity NIF)
OU, Organization Unit	Organization Unit	“Certificat d’aplicació”
SN, Serial Number	CIF	Public Administration, organ or public entity CIF.
CN, Common Name	Name of the application or system	e. g. “PLATAFORMA DE VALIDACIÓN DE L’AJUNTAMENT DE xxx”
C, Country	Country	C= ES.

4.2.2. Certificate Extension

Extension	Critic	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Key Usage	Yes	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	Email protection TLS Web Client Authentication
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question >
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Yes	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-eseal 0.4.0.1862.1.6.2

X509v3 Certificate Policies	-	<OID of the certification policy corresponding to the certificate> 1.3.6.1.4.1.15096.1.3.2.91.1 <URI of the DPC> User Notice: "Certificat d'aplicació. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" < OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-l> 0.4.0.194112.1.1
X509v3 Subject Alternative Name	-	rfc822Name: contact mail (optional)

4.3. Profile of the Electronic Office Certificate (Seu-e nivell mig)

4.3.1. Certificate

DN Field	Value	Description
CN, Common Name	Name	Name of domain name where the certificate will be gathered. Shall be coincident with the one in the extension Subject Alternative Names
O, Organization	Corporate name	Denomination ("official" name of the organization) of the certification services subscriptor.
OU, Organizational Unit	Organizational Unit	*"Mid-level Electronic Seal Certificate"*
OU, Organizational Unit	Organizational Unit	*Descriptive name of the location.*
SN, SerialNumber	CIF	*Shall contain the NIF of the electronic site responsible entity.*
OrganizationIdentifier		Organization identifier According to the technical standard ETSI EN 319 412-1 (VATES + NIF of the entity)
businessCategory	"Government Entity"	Business Category
C, Country	Country	*C=ES*

jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	Country	Subject Jurisdiction of Incorporation or Registration *C=ES*
L, Locality	Locality	Locality
S, State or Province	Region	Region

4.3.2. Certification Extension

Extension	Critic	Values
X509v3 Authority Key Identifier	-	<id of the public key of the CA, obtained from the hash of the public key in question>
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question >
X509v3 Key Usage	Yes	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	TLS web Server authentication
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 Certificate Policies	-	<OID associated with the DPC> 1.3.6.1.4.1.15096.1.3.2.5.2 <URI of the DPC> User Notice: “Certificat de seu electrònica de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A” <OID asociado a los certificados de sede de nivel medio / sustancial> 2.16.724.1.3.5.5.2 <OID ETSI QCP-w> 0.4.0.194112.1.4

Qualified Certificate Statements		Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-web 0.4.0.1862.1.6.3
X509v3 Subject Alternative Name	-	dNSName: domain name where the certificate will be hosted

4.4. Profile of the Secure Server Certificates (Dispositiu SSL)

4.4.1. Certificates

DN Fields°	Value	Description
CN, Common Name	Name	(BR. 7.1.4.2.2.a) This domain shall be coincident with the one indicated (o with one of them) in Subject Alt Names).
O, Organization	Corporate name	Denomination (“official” name of the organization) of the certification services subscriber.
OU, Organizational Unit (Optional)	Organization Unit	*Descriptive name of the department*
OrganizationIdentifier		Organization Identifier According to the technical standard ETSI EN 319 412-1 (VATES + NIF of the entity)
L, Locality	Locality	(BR. 7.1.4.2.2.e) Indication required when existing field Organization(O)
C, Country	Country	2 characters country code according to the standard ISO 3166-1. By default “ES”. (BR. 7.1.4.2.2.h) Indication required when existing field Organization (O)

The characters (BR.X) are requirements from the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* from the CA/Browser Forum, in line with the current version in the moment of publication of this profile.

4.4.2. Certificates Extension

Extension	Critic	Values
X509v3 Subject Alternative Name	-	URL, domain name or device identification or service holding the keys or the application.
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Key Usage	Yes	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	Server Authentication (1.3.6.1.5.5.7.3.1)
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method 1: Id-ad-ocsp (1.3.6.1.5.5.7.48.1) Access Location 1: <URI to access the OCSP service> Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2) Access Location 2: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Certificate Policies	-	<OID of the Certification policy corresponding to the certificate> 1.3.6.1.4.1.15096.1.3.2.51.1 <URI of the CPS> User Notice: “Certificat de dispositiu SSL. Adreça i NIF of the provider: Via Laietana 26 08003 Barcelona Q0801175A”
X509v3 Subject Alternative Name	-	dNSName: domain name where the certificate will be hosted.

4.5. Profile of the Secure Server Certificate Extended Validation (Dispositiu SSL EV)

4.5.1. Certificate

DN Field	Value	Description
CN, Common Name	Name	(EVG 9.2.3) Name of a single domain name (BR. 7.1.4.2.2.a) This domain shall be coincident with the one indicated (or one of them) in Subject Alt Names).
O, Organization	Corporate name	Official name of the organization subscribing the certificate.
OU, Organizational Unit (Optional)	Organization Unit	*Descriptive name of the department*
SN, SerialNumber	CIF	CIF of the organization subscribing the certificate. (EVG 9.2.6) Registration Number
OrganizationIdentifier		Organization identifier According to the technical standard ETSI EN 319 412-1 (VATES + NIF of the entity)
businessCategory	"Government Entity"	(EVG 9.2.4) Business Category
C, Country	Country	2 characters country code according to ISO 3166-1. By default "ES".(EVG 9.2.7) Country (required) (BR. 7.1.4.2.2.h) indication required existing the field Organization (O)
L, Locality		(EVG 9.2.7) Address of Place of Business: City (required) (BR. 7.1.4.2.2.e) indication required existing the field Organization (O)
jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	Country	(EVG 9.2.5) Subject Jurisdiction of Incorporation or Registration

The characters (BR.X) are requirements from the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* from the CA/Browser Forum, in line with the current version in the moment of publication of this profile.

The characters (EVG 9.2.X) are specific requirements for certificates *Extended Validation* according to CA/Browser Forum in the *Guidelines For The Issuance And Management Of Extended Validation Certificates*, in line with the current version in the moment of publication of this profile.

4.5.2. Certificates extensions

Extension	Critic	Values
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question >
X509v3 Key Usage	Yes	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	Server Authentication (1.3.6.1.5.5.7.3.1)
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access the OCSP service> Access Method: Id-ad-caIssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 Certificate Policies	-	<OID associated with the DPC> 1.3.6.1.4.1.15096.1.3.2.51.2 <URI of the DPC> User Notice: “Certificat de dispositiu SSL EV. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A” <OID ETSI QCP-w> 0.4.0.194112.1.4
Qualified Certificate Statements		Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-web 0.4.0.1862.1.6.3

X509v3 Subject Alternative Name	-	dNSName: Domain name where the certificate will reside

4.6. Profile of the Qualified Time Stamp Certificates

4.6.1. Certificate

Field of the DN	Value	Description
CN, Common Name	Name	*Shall contain a TSU identifier that uniquely identifies the relevant TSU, including the client reference.*
O, Organization	Organization	Consorci Administració Oberta de Catalunya
OI, Organization Identifier	Organization identifier	"VATES-Q0801175A"
C, Country	Country	C=ES

4.6.2. Certificate Extensions

Extension	Critics	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Key Usage	Yes	digitalSignature contentCommitment
X509v3 Extended Key Usage	Yes	id-kp-timeStamping {1.3.6.1.5.5.7.3.8}
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Certificate Policies	-	<OID associated with the DPC> 1.3.6.1.4.1.15096.1.3.2.111 <URI de la PC>https://www.aoc.cat/catcert/regulacio userNotice: "Certificat de Servei Segur de TSA qualificada"

id-ce-privateKeyUsagePeriod 2.5.29.16		*Has the aim to limit the validity of the private key: 3 years*
Authority Information Access	-	accessMethod: Id-ad-caIssuers accessLocation: <URI of access to the certificate of the issuer CA> accessMethod: Id-ad-ocsp accessLocation: <URI to access the OCSP service>

The qualified Tokens of Timestamp, should include an instance of the extension Statements according to the syntax defined in IETF RFC 3739 [i.3], provision 3.2.6.

The extension should include an instance of "esi4-qtstStatement-1" as provided by Annex B of the standard ETSI TS 319 422 .