



**Administració
Oberta de
Catalunya**

**Profile description of
Consorci AOC Certificates**

Reference: D1111_E0650_Perfils_de_Certificats
Version: 7.2
Date: 09/03/2025

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://epsd.aoc.cat/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 multi-domain 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 issuance of the subscriber identification document"	31/03/2022
6.7	Review without changes	29/03/2023
6.8	- Eliminated references to QWAC and QTSA. - Change URLs of regulation and CRL. - Marked QCStatements extension as not critical.	10/05/2023
6.9	- Section 2.7: Inclusion of T-CATP pseudonym. - Removed direction and NIF from the extension of certificate profiles. - Removed email protection from Extended Key Usage (EKU) and rfc822. Adobe Authentic Documents Trust extension inclusion.	15/11/2023
6.10	Section 2.7: T-CATP pseudonym profile adjustments	22/05/2024
7.0	Inclusion of the new AOC G3 hierarchy. It is numbered as version 7.0 for the purposes of document management	31/10/2024
7.1	Section 4.3: Inclusion of the Qualified Time-Stamp Service Certificate profile.	18/12/2024

7.2	• Removed the inclusion of the DNI in the Surname • Removed the KU Key Encipherment within the natural person certificates • Removed the Adobe EKU within the web authentication certificates • Inclusion of a DN within the SAN in order to separate the surnames in the natural person linked to a legal person certificate, the natural person representative of a legal person certificate and the public employee certificate	09/03/2025
-----	---	------------

Table of contents

1. Introduction	6
2. Description of the profiles of personal certificates of the public sector	7
2.1. Profile of the high-level authentication certificate for public employee (T-CAT autenticació)	7
2.1.1. Certificate	7
2.1.2. Extensions	8
2.2. Profile of the mid-level qualified certificates of authentication and signature for public employee(T-CATP)	9
2.2.1. Certificate	9
2.2.2. Extensions	10
2.3. Profile of the authentication and signature certificate for mid-level associated persons (T-CATP persona vinculada)	11
2.3.1. Certificate	11
2.3.2. Extensions	12
2.4. Profile of the authentication and signature certificate for high-level associated persons (T-CATP persona vinculada)	13
2.4.1. Certificate	13
2.4.2. Extensions	14
2.5. Profile of high-level authentication certificate for public employee with pseudonyms (T-CAT pseudònim autenticació)	15
2.5.1. Certificates	15
2.5.2. Extensions	16
2.6. Profile of the signature certificates for high-level public employees with pseudonyms (T-CAT pseudònim signatura)	17
2.6.1. Certificate	17
2.6.2. Extensions	18
2.7. Profile of the authentication and signature mid-level/substantial certificate qualified for public employees with pseudonyms (T-CATP pseudònim).	19
2.7.1. Certificate	19
2.7.2. Extensions	20
2.8. Profile of the authentication and signature certificate for representatives acting before the Public Administrations (T-CAT representant)	21
2.8.1. Certificate	21
2.8.2. Common name	22
2.8.3. Extensions	23
2.9. Profile of high-level signature certificate for public employee (T-CAT signatura)	24
2.9.1. Certificate	24
2.9.2. Extensions	25
2.10. Profile of the Authentication Certificates and signature of public worker of medium level (T-CATP Treballador públic)	26
2.10.1. Certificate	26
2.10.2. Extensions	27

2.11. Profile of High Level Public Worker Authentication and Signature Certificates (T-CAT Public Treballador)	28
2.11.1. Certificate	28
2.11.2. Extensions	29
3. Description of Citizenship Certificate Profiles	30
3.1. Profiles of Citizenship Certificates (idCAT certificat)	30
3.1.1. Certificates	30
3.1.2. Certificates extension	31
4. Description of certification for Devices and Infrastructure Profiles	32
4.1. Profile of Advanced Electronic Seal Certificate (Segell nivell mig)	32
4.1.1. Certificate	32
4.1.2. Certificates extension	33
4.1.3. Mid-level Extensions	34
4.2. Profile of the Application Certificates (Dispositiu aplicació)	35
4.2.1. Certificate	35
4.2.2. Certificate Extension	36
4.3. Qualified Time-Stamp Certificate profile	37
4.3.1. Certificate	37
4.3.2. Qualified certificates extensions	38

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://epsd.aoc.cat /regulacio](https://epsd.aoc.cat/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 autenticació)

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.
Serialnumber	NIF	Signatory Identification document number, with the semantic proposed by the standard ETSI EN319412-1 ¹
SN, Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, ...)
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)+ 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-99949992L. 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-calssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	<CRL's URI>
X509v3 Key Usage	Yes	Digital Signature
X509v3 Extended Key Usage		Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associated with the CPS> 1: 1.3.6.1.4.1.15096.1.3.2.7.1.2 <URI of the CPS> <User Notice> " Certificat electrònic d'empleat públic de nivell alt d'autenticació <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) 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.
Serialnumber	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN319412-1 ²
SN, Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, ...)
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)+ 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-99949992L. 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-calssuers Access Location: <URI of the certificate of the sender EC>
X509v3 CRL Distribution Points	-	<CRL's URI>
X509v3 Key Usage	Yes	Digital Signature Content Commitment
X509v3 Extended Key Usage		Client Authentication Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID of the CPS> 1.3.6.1.4.1.15096.1.3.2.7.3.1 <URI of the CPS> <User Notice> "Certificat electrònic d'empleat públic de nivell mig" <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: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Subject Alternative Name	-	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.
Serialnumber	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN 319 412-1 ³
SN, Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, ...)
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)+ 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-99949992L. 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-calssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	<CRL's URI>
X509v3 Key Usage	Yes	Digital Signature Content Commitment
X509v3 Extended Key Usage		Client Authentication Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID of the CPS> 1.3.6.1.4.1.15096.1.3.2.86.1 <URI of the CPS> <User Notice> "Certificat electrònic de persona vinculada de nivell mig." <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: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Subject Alternative Name		DirectoryName: OID: 1.3.6.1.4.1.15096.0.1 = "Name of the natural person linked to the legal person" OID: 1.3.6.1.4.1.15096.0.2 = "Primer surname of the natural person linked to the legal person" OID: 1.3.6.1.4.1.15096.0.3 = "Second surname of the natural person linked to legal person"

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.
Serialnumber	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN 319 412-1 ⁴ shall preferably apply.
SN, Surname	Surname (natural person)	First and second surname (according the Identification Document - DNI/Passport, ...)
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-99949992L. 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-calssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	<CRL's URI>
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-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType 0.4.0.1862.1.6.1
X509v3 Key Usage	Yes	Digital Signature Content Commitment
X509v3 Extended Key Usage		Client Authentication SmartCardLogon Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID associated with the CPS> 1.3.6.1.4.1.15096.1.3.2.82.1 <URI of the CPS> User Notice: "Certificat electrònic de persona vinculada de nivell alt." <OID of the certification policy ETSI: QCP-n-qscd> 0.4.0.194112.1.2
X509v3 Subject Alternative Name	-	(optional) otherName-userPrincipalName (UPN): User in Windows' domain of the key holder. DirectoryName: OID: 1.3.6.1.4.1.15096.0.1 = "Nom del representant" OID: 1.3.6.1.4.1.15096.0.2 = "Primer cognom del representant" OID: 1.3.6.1.4.1.15096.0.3 = "Segon cognom del representant"

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

2.5.1. Certificates

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 d'autenticació"
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	Title/PSEUDONIM + " - " + NIP + " - " + Organization (AUT) Ex: SUBINSPECTOR - NIP 11111111 - ORGANITZACIÓ DE PROVES (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-calssuers Access Location: <URL of the CA certificate location.>
X509v3 CRL Distribution Points	-	<CRL's URI>
X509v3 Key Usage	Yes	Digital Signature
X509v3 Extended Key Usage		Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associated with the CPS> 1.3.6.1.4.1.15096.1.3.2.4.1.2 <URI of the CPS> User Notice: "Certificat electrònic d'mpleat públic amb pseudònim de nivell alt d'autenticació." <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	Title/PSEUDONIM + " - " + NIP + " - " + Organization (SIG) Ex: SUBINSPECTOR - NIP 11111111 - ORGANITZACIÓ DE PROVES (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-calssuers Access Location: <URL of the CA certificate location.>
X509v3 CRL Distribution Points	-	<CRL's URI>
X509v3 Certificate Policies	-	<OID de la CPS correspondiente> 1.3.6.1.4.1.15096.1.3.2.4.1.1 <URI of the CPS> User Notice: " Certificat qualificat de signatura d'empleat públic amb pseudònim de nivell alt." <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	-	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: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Yes	Content commitment
X509v3 Extended Key Usage	-	Adobe Authentic Documents Trust
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 mid-level/substantial certificate qualified for public employees with pseudonyms (T-CATP pseudònim).

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	"Empleat públic amb pseudònim de nivell mig."
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	Title/PSEUDONIM + " - " + NIP + " - " + Organization (TCAT) Ex: SUBINSPECTOR - NIP 11111111 - ORGANITZACIÓ DE PROVES (TCAT)
C, Country	País	C = "ES"

2.7.2. 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-calssuers Access Location: <URL of the CA certificate location.>
X509v3 CRL Distribution Points	-	<CRL's URI>
X509v3 Certificate Policies	-	<OID de la CPS corresponente> 1.3.6.1.4.1.15096.1.3.2.4.2 <URI of the CPS> User Notice: "Certificat qualificat empleat públic amb pseudònim de nivell mig" <OID associated with high-level certificate for public servant with pseudonym> 2.16.724.1.3.5.4.2 < 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: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Yes	Digital Signature Content commitment
X509v3 Extended Key Usage	-	Client Authentication Adobe Authentic Documents Trust
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.4.2.1 = "Certificat electrònic empleat públic amb pseudònim de nivell mig" OID: 2.16.724.1.3.5.4.2.2 = <O of DN> OID: 2.16.724.1.3.5.4.2.3 = <CIF of subscriber entity>

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

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	"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.
Serialnumber	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN319412-1 ⁵
SN, 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: "99949992L Nomdos Especimendos Especimendos (R: Q0000000J)"
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-Q0000000J)
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: NOMDOS SPECIMENDOS SPECIMENDOS /Protocol number: XXX /Fecha Otorgamiento: dd-mm-aaaa In Official Journals: Boletín: XXX /Fecha: dd-mm-aaaa /Número resolución: XXX

⁵ Serial Number = e. g: IDCES-99949992L. 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. Common name

Field	Content	Example	Size (*)
NIF	DNI Number	99949992L	10
Name	According to the Identification Document	Nomdos	
Surname 1	According to the Identification Document	Specimendos	
Literal	(R:		4
NIF of the represented entity.	NIF of the represented entity, as established in official registers.	Q0000000J	9
Literal	)		2

(*) counting subsequent blank space.

2.8.3. 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-calssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	<CRL's URI>
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 CPS> User Notice: "Certificat electrònic de representant davant les AAPP de nivell alt." <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	-	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: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Yes	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	Client Authentication SmartCardLogon Adobe Authentic Documents Trust
X509v3 Subject Alternative Name	-	(optional) otherName-userPrincipalName (UPN): User in Windows' domain of the key holder. DirectoryName: OID: 1.3.6.1.4.1.15096.0.1 = "Nom del representant" OID: 1.3.6.1.4.1.15096.0.2 = "Primer cognom del representant" OID: 1.3.6.1.4.1.15096.0.3 = "Segon cognom del representant"

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

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 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.
Serialnumber	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN319412-1 ⁶
SN, Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, ...)
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-99949992L. 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

Extension	Critics	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-calssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	<CRL's URI>
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-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Yes	Content Commitment
X509v3 Extended Key Usage	-	Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID associated with the CPS> 1.3.6.1.4.1.15096.1.3.2.7.1.1 <URI of the CPS> User Notice: " Certificat qualificat de signatura d'empleat públic de nivell alt." <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>

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

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 mig"
Title (optional)	Title	Shall include the title that links the natural person to the administration, organism or public entity subscribing the certificate.
Serialnumber	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN319412-1 ⁷
SN, Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, ...)
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-99949992L. 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

Extension	Critics	Values
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 to access the OCSP service > Access Method: Id-ad-calssuers Access Location: < URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	<CRL's URI>
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	Client Authentication Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID associated with the CPS> 1.3.6.1.4.1.15096.1.3.2.86.3 <URI of the CPS> <User Notice> "Certificat electrònic de treballador públic de nivell mig." <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: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Subject Alternative Name	-	directoryName: OID: 1.3.6.1.4.1.15096.0.1 = "Nom del treballador públic" OID: 1.3.6.1.4.1.15096.0.2 = "Primer cognom del treballador públic" OID: 1.3.6.1.4.1.15096.0.3 = "Segon cognom del treballador públic"

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

2.11.1. 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.
Serialnumber	NIF	Identification document signatory number, with the semantic proposed by the standard ETSI EN319412-1 ⁸
SN, Surname	Surname (natural person)	First and second surname (according to the Identification Document - DNI/Passport, ...)
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-99949992L. 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

2.11.2. Extensions

Extension	Critics	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 to the OCSP service> Access Method: Id-ad-caIssuers Access Location: < URI of the certificate of the issuer EC >
X509v3 CRL Distribution Points	-	<CRL's URI>
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-QcSSCD 0.4.0.1862.1.4 Id-etsi-qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi-qcs-QcType 0.4.0.1862.1.6.1
X509v3 Key Usage	Yes	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	Client Authentication SmartCardLogon Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID associated with the CPS> 1.3.6.1.4.1.15096.1.3.2.82.2 <URI of the CPS> User Notice: "Certificat electrònic de treballador públic de nivell alt." <OID of the certification policy ETSI: QCP-n-qscd> 0.4.0.194112.1.2
X509v3 Subject Alternative Name	-	(optional) otherName-userPrincipalName (UPN):Windows domain user of the key holder directoryName: OID: 1.3.6.1.4.1.15096.0.1 = "Nom del treballador públic" OID: 1.3.6.1.4.1.15096.0.2 = "Primer cognom del treballador públic" OID: 1.3.6.1.4.1.15096.0.3 = "Segon cognom del treballador públic"

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: NOMDOS SPECIMENDOS SPECIMENDOS – DNI 99949992L
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 issuance 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 Content Commitment
X509v3 Extended Key Usage	-	TLS Web Client Authentication Adobe Authentic Documents Trust
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	-	<CRL's URI>
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 CPS> User Notice: "idCAT Certificat" <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 : <URI de la PDS> https://www.aoc.cat/catcert/pds_enId-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-calssuers 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

DN field	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"
Serialnumber	CIF	Public Administration, organ or public entity CIF.
SN, Surname (Optional)	Surname (Natural Person)	First and second surname (according the Identification Document -DNI/Passport, ...)
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 VALIDACIÓ 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	-	TLS Web Client Authentication Adobe Authentic Documents Trust
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	-	<CRL's URI>
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: <URI de la PDS> 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 CPS> User Notice: "Certificat de segell electrònic nivell mig." <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-I> 0.4.0.194112.1.1
X509v3 Subject Alternative Name	-	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"
Serialnumber	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	-	TLS Web Client Authentication Adobe Authentic Documents Trust
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-calssuers Access Location: <URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	<CRL's URI>
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: <URI de la PDS> 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 CPS> User Notice: "Certificat d'aplicació." < OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-I> 0.4.0.194112.1.1

4.3. Qualified Time-Stamp Certificate profile

4.3.1. Certificate

DN Fields	Name	Description
O, Organization	Organization	Consorti Administració Oberta de Catalunya
Organization Identifier		Organization identifier different of the name as specified in the technical standard ETSI EN 319 412-1 (VATES + NIF of the entity)
CN, Common Name	Name	<i>CONSORCI AOC Q TSU + "year of the issuance"</i>
C, Country	Country	C = "ES"

4.3.2. Qualified certificates extensions

Extension	Critical	Values
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	Sí	Time Stamping
X509v3 Subject Key Identifier	-	<certificate public key id, obtained from a hash of the public key>
X509v3 Authority Key Identifier	-	<CA certificate public key id, obtained from a hash of the public key>
X509v3 CRL Distribution Points	-	<CRL URI>
X509v3 Certificate Policies	-	<OID associated to the CPS> 1.3.6.1.4.1.15096.1.3.2.112 <CPS URI> User Notice: "Qualified Time-Stamp Certificate Service" < OID "for EU qualified certificates issued to legal persons" in accordance with ETSI EN 319 411-2: QCP-> 0.4.0.194112.1.1
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: <PDS URI> Id-etsi- qcs-QcType-eseal 0.4.0.1862.1.6.2
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI to access to the OCSP service> Access Method: Id-ad-calssuers Access Location: <URL to the CA certificate location>
Private Key Usage Period		<Validity starting date and validity finishing date, maximum 2 years>