



**Administració
Oberta de
Catalunya**

**Descripció dels perfils de Certificats
Consorti AOC**

Referència: D1111_E0650_Perfils_de_Certificats
Versió: 7.2
Data: 09/03/2025

La versió original en vigor d'aquest document es troba en format electrònic publicada en el lloc web del Consorci AOC i pot ser accessible a través de la següent URL:
<https://epsd.aoc.cat/regulacio/>

Historial de versions

Versió	Resum dels canvis	Data
5.0	Adaptació a EIDAS	9/5/2018
6.0	Unificació en un únic document del document de perfils emesos per EC-SECTORPUBLIC i EC-CIUTADANIA.	26/07/2018
6.1	- Revisió anual de la documentació, post auditoria eIDAS. "4.4. Perfil dels Certificats de Servidor Segur (Dispositiu SSL)": eliminada opció de multidominio o wildcard.	24/07/2019
6.2	"2.6: Perfil dels certificats de signatura d'empleat públic amb pseudònim nivell alt": Inclusió d'EKU "2.8. Perfil dels certificats de signatura d'empleat públic de nivell nivell alt": Inclusió d'EKU	31/3/2020
6.3	Inclusió de certificats d'autenticació i signatura de treballador públic de nivell mitjà i de nivell alt	03/08/2020
6.4	Revisió del Document	27/01/2021
6.5	Revisió del Document	20/07/2021
6.6	"3.1.1 Certificat": Alteració en descripció: C = "País d'expedició del document identificatiu del subscriptor."	31/03/2022
6.7	Revisió sense canvis.	29/03/2023
6.8	- Eliminades referències a QWAC y QTSA. - Canvi URLs de regulació y CRL. - Marcada extensió QCStatements com a no crítica.	10/05/2023
6.9	- Apartat 2.7: Inclusió de T-CATP pseudònim. - Eliminació de la direcció i el NIF de les extensions dels perfils de certificat. - Eliminació del email protection del Extended Key Usage (EKU) i Rfc822. Inclusió extensió Adobe Authentic Documents Trust.	15/11/2023
6.10	Apartat 2.7: Ajusts perfil T-CATP pseudònim	22/05/2024
7.0	Inclusió de la nova jerarquia AOC G3. Es numera com a versió 7.0 a l'efecte de gestió documental.	31/10/2024
7.1	Secció 4.3: Inclusió del perfil dels Certificats de Segell de Temps Qualificats.	18/12/2024

7.2	• Eliminació de la inclusió del DNI al Surname • Als certificats de persona física eliminació del KU Key Encipherment • Als certificats d'autenticació eliminació de l'EKU d'Adobe. • Als certificats de persona vinculada, representant i treballador públic s'afegix un DN al SAN per la separació dels cognoms	09/03/2025
-----	--	------------

Índex

1. Introducció	6
2. Descripció de Perfils de Certificats Personals del Sector Públic	7
2.1. Perfil dels Certificats d'autenticació de empleat públic de nivell alt (T-CAT autenticació)	7
2.1.1. Certificat	7
2.1.2. Extensions	8
2.2. Perfil dels Certificats qualificat d'autenticació i signatura de empleat públic de nivell mitjà (T-CATP)	9
2.2.1. Certificat	9
2.2.2. Extensions	10
2.3. Perfil dels Certificats d'autenticació i signatura de persona vinculada de nivell mitjà (T-CATP persona vinculada)	11
2.3.1. Certificat	11
2.3.2. Extensions	12
2.4. Perfil dels Certificats d'autenticació i signatura de persona vinculada de nivell alt (T-CAT persona vinculada)	13
2.4.1. Certificat	13
2.4.2. Extensions	14
2.5. Perfil dels Certificats d'autenticació de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim autenticació)	15
2.5.1. Certificat	15
2.5.2. Extensions	16
2.6. Perfil dels Certificats de signatura de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim signatura)	17
2.6.1. Certificat	17
2.6.2. Extensions	18
2.7. Perfil dels Certificats qualificats d'autenticació i signatura d'empleat públic amb pseudònim de nivell mig (T-CATP pseudònim)	19
2.7.1. Certificat	19
2.7.2. Extensions	20
2.8. Perfil dels Certificats d'autenticació i signatura de representant davant les Administracions Públiques (T-CAT representant)	21
2.8.1. Certificat	21
2.8.2. Common name	22
2.8.3. Extensions	23
2.9. Perfil dels Certificats de signatura de empleat públic de nivell alt (T-CAT signatura)	24
2.9.1. Certificat	24
2.9.2. Extensions	25
2.10. Perfil dels Certificats d'autenticació i signatura de treballador públic de nivell mitjà (T-CATP Treballador públic)	26
2.10.1. Certificat	26
2.10.2. Extensions	27

2.11. Perfil dels Certificats d'autenticació i signatura de treballador públic de nivell alt (T-CAT Treballador públic)	28
2.11.1. Certificat	28
2.11.2. Extensions	29
3. Descripció de Perfils de Certificats de Ciutadania	30
3.1. Perfil dels Certificats de Ciutadà (idCAT certificat)	30
3.1.1. Certificat	30
3.1.2. Extensions dels certificats	31
4. Descripció dels Perfils de Certificats de Dispositius i Infraestructura	32
4.1. Perfil dels Certificats de Segell Electrònic Avançat (Segell nivell mig)	32
4.1.1. Certificat	32
4.1.2. Extensions dels certificats	33
4.1.3. Extensions de nivell mitjà	34
4.2. Perfil dels Certificats d'Aplicació (Dispositiu aplicació)	35
4.2.1. Certificat	35
4.2.2. Extensions dels certificats	36
4.3. Perfil dels Certificats de Segell de Temps Qualificats	37
4.3.1. Certificat	37
4.3.2. Extensions dels certificats qualificats	38

1. Introducció

Aquest document de Descripció dels perfils de certificats té per objecte detallar el contingut dels certificats emesos pel Consorci AOC, en virtut dels requisits establerts a aquests efectes pel Ministeri competent en serveis electrònics de confiança; és a dir, especifica quina és la configuració (principalment, Camp del DN, Nom i Descripció) i l'extensió (Extensió, Crítica –si/no-, i Valors) dels certificats personals de empleat públic, certificats de ciutadans i certificats de Dispositius i Infraestructura, cada un d'ells amb una Política de certificació pròpia (accessibles des de la URL <https://epsd.aoc.cat/regulacio>). També fa referència a la composició del camp Common Name (CN) en el cas d'aquells certificats que en disposin.

La seva emissió s'ha efectuat tenint en compte les disposicions del Reglament (UE) 910/2014 del Parlament Europeu i del Consell de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques al mercat interior i pel qual es deroga la Directiva 1999/93/CE (d'ara endavant, eIDAS). També s'ha seguit com a referència el document "*Perfiles de certificados electrónicos*", 1a edició electrònica d'abril de 2016 i disponible esta publicació en el Portal de Administración Electrónica (PAe): <http://administracionelectronica.gob.es/>.

2. Descripció de Perfils de Certificats Personals del Sector Públic

2.1. Perfil dels Certificats d'autenticació de empleat públic de nivell alt (T-CAT autenticació)

2.1.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme o entitat de dret públic subscriptora del certificat, a la qual es troba vinculat l'empleat.
OU, Organization Unit	Unitat en la organització	"Empleat públic de nivell alt d'autenticació"
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física, que la vincula amb l'administració, organisme o entitat de dret públic subscriptora del certificat.
Serial Number	NIF	Número del document d'identitat del signatari amb la semàntica proposta per la norma ETSI EN 319 412-1 ¹
SN, Surname	Cognoms (persona física)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI / Passaport, ...)
Given name	Nom	Nom, d'acord amb el document d'identitat (DNI, passaport,...)
CN, Common Name	Nom, cognoms i NIF	Nom i dos cognoms d'acord amb el document d'identitat (DNI / passaport) + NIF de l'empleat públic + " (AUT)"
C, Country	País	C = "ES"
Organization Identifier		Segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat)

¹ SerialNumber = p. ex: IDCES-99949992L. 3 caràcters per indicar el tipus de document (IDC= document nacional d'identitat, PAS=pasaport, ...) + 2 caràcters per identificar el país (ÉS) + Nombre d'identitat (Printable String)) Size [RFC 5280] 64

2.1.2. Extensions

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la CA, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificat de l'EC emissora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Key Usage	Sí	Digital Signature
X509v3 Extended Key Usage	-	Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associat a la DPC> 1: 1.3.6.1.4.1.15096.1.3.2.7.1.2 <URI de la DPC> <User Notice> " Certificat electrònic d'empleat públic de nivell alt d'autenticació. <OID de la política de certificació d'empleat públic de nivell alt> 2.16.724.1.3.5.7.1 <OID de la política de certificació ETSI: NCP+> 0.4.0.2042.1.2
X509v3 Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuari en el domini Windows del posseïdor de claus 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 del DN> OID: 2.16.724.1.3.5.7.1.3 = <CIF de l'entitat subscriptora> OID: 2.16.724.1.3.5.7.1.4 = <serialNumber del DN> OID: 2.16.724.1.3.5.7.1.6 = <Given name> OID: 2.16.724.1.3.5.7.1.7 = <Primer cognom del empleat públic> OID: 2.16.724.1.3.5.7.1.8 = <Segon cognom del empleat públic>

2.2. Perfil dels Certificats qualificat d'autenticació i signatura de empleat públic de nivell mitjà (T-CATP)

2.2.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme o entitat de dret públic subscriptora del certificat, a la qual es troba vinculat l'empleat.
OU, Organization Unit	Unitat en la organització	"Empleat públic de nivell mig"
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física, que la vincula amb l'administració, organisme o entitat de dret públic subscriptora del certificat.
Serial Number	NIF	Número del document d'identitat del signatari, amb la semàntica proposta per la norma ETSI EN 319 412-1 ²
SN, Surname	Cognoms (persona física)	Primer i segon cognom (d'acord amb el document d'identitat – DNI / Passaport, ...)
Given name	Nom	Nom, d'acord amb el document d'identitat (DNI, passaport, ...)
CN, Common Name	Nom, cognoms i NIF	Nom i dos cognoms d'acord amb el document d'identitat (DNI / Passaport) + NIF de l'empleat públic + " (TCAT)"
C, Country	País	C = "ES"
Organization Identifier		Segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat)

² SerialNumber = p. ex: IDCES-99949992L. 3 caràcters per indicar el tipus de document (IDC= document nacional d'identitat, PAS = passaport, ...) + 2 caràcters per identificar el país (ÉS) + Nom d'identitat (Printable String)) Size [RFC 5280] 64

2.2.2. Extensions

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la CA, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acces al servei OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificat de l'EC emissora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage		Client Authentication Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID de la DPC> 1.3.6.1.4.1.15096.1.3.2.7.3.1 <URI de la DPC> <User Notice> Certificat electrònic de empleat públic de nivell mig. <OID que indica certificat d'empleat públic de nivell mitjà> 2.16.724.1.3.5.7.2 <OID de la política de certificació 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 anys 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 mitjà" OID: 2.16.724.1.3.5.7.2.2 = <O del DN> OID: 2.16.724.1.3.5.7.2.3 = <CIF de l'entitat subscriptora> OID: 2.16.724.1.3.5.7.2.4 = <serialNumber del DN> OID: 2.16.724.1.3.5.7.2.6 = <Given name> OID: 2.16.724.1.3.5.7.2.7 = <Primer cognom de l'empleat públic> OID: 2.16.724.1.3.5.7.2.8 = <Segon cognom de l'empleat públic> OID: 2.16.724.1.3.5.7.2.9 = <correu electrònic de l'empleat públic>

2.3. Perfil dels Certificats d'autenticació i signatura de persona vinculada de nivell mitjà (T-CATP persona vinculada)

2.3.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme o entitat de dret públic subscriptora del certificat, a la qual es troba vinculat l'empleat.
OU, Organization Unit	Unitat en la organització	"Persona vinculada de nivell mig"
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física, que la vincula amb l'administració, organisme o entitat de dret públic subscriptora del certificat.
Serial Number	NIF	Número del document d'identitat del signatari, amb la semàntica proposta per la norma ETSI EN 319 412-1 ³
SN, Surname	Cognoms (persona física)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI / Passaport, ...)
Given name	Nom	Nom, d'acord amb el document d'identitat (DNI, passaport, ...)
CN, Common Name	Nom, cognoms i NIF	Nom i dos cognoms, d'acord amb el document d'identitat (DNI / Passaport) + NIF de l'empleat públic + " (TCAT)"
C, Country	País	C = "ES"
Organization Identifier		Segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat)

³ SerialNumber = p. ex: IDCES-99949992L. 3 caràcters per indicar el tipus de document (IDC= document nacional d'identitat, PAS=passaport, ...) + 2 caràcters per identificar el país (ÉS) + Nom d'identitat (Printable String)) Size [RFC 5280] 64

2.3.2. Extensions

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtinguda a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la CA, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificat de l' EC emissora>
X509v3 CRL Distribution Points	-	<URI de la CRL>I
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	Client Authentication Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID de la DPC> 1.3.6.1.4.1.15096.1.3.2.86.1 <URI de la DPC> <User Notice> " Certificat electrònic de persona vinculada de nivell mig." <OID de la política de certificació 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 anys 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 de la persona vinculada" OID: 1.3.6.1.4.1.15096.0.2 = "Primer cognom persona vinculada" OID: 1.3.6.1.4.1.15096.0.3 = "Segon cognom persona vinculada"

2.4. Perfil dels Certificats d'autenticació i signatura de persona vinculada de nivell alt (T-CAT persona vinculada)

2.4.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme o entitat de dret públic subscriptora del certificat, a la qual es troba vinculada la persona.
OU, Organization Unit	Unitat a l'organització	"Persona vinculada de nivell alt"
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física, que ho vincula amb l'administració, organisme o entitat de dret públic subscriptora del certificat.
Serial Number	NIF	Número del document d'identitat del signatari, amb la semàntica proposta per la norma ETSI EN 319 412-1 ⁴
SN, Surname	Cognoms (persona física)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI, Passaport, ...)
Given name	Nom	Nom de pila, d'acord amb el document d'identitat (DNI, passaport, ...)
CN, Common Name	Nom, cognoms i NIF	Nom i dos cognoms, d'acord amb el document d'identitat (DNI / Passaport) + NIF de la persona vinculada + " (TCAT)"
C, Country	País	C = "ES"
Organization Identifier		Segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat)

⁴ SerialNumber = p. ex: IDCES-99949992L. 3 caràcters per indicar el tipus de document (IDC= document nacional d'identitat) + 2 caràcters per identificar el país (ÉS) + Número d'identitat (Printable String)) Size [RFC 5280] 64

2.4.2. Extensions

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la CA, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificat de l'EC emissora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	-	Id-etsi-qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi-qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys 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	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	Client Authentication SmartCardLogon Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.82.1 <URI de la DPC> User Notice: "Certificat electrònic de persona vinculada de nivell alt." <OID de la política de certificació ETSI: QCP-n-qscd> 0.4.0.194112.1.2
X509v3 Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuari en el domini Windows del posseïdor de claus directoryName: OID: 1.3.6.1.4.1.15096.0.1 = "Nom de la persona vinculada" OID: 1.3.6.1.4.1.15096.0.2 = "Primer cognom de la persona vinculada" OID: 1.3.6.1.4.1.15096.0.3 = "Segon cognom de la persona vinculada"

2.5. Perfil dels Certificats d'autenticació de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim autenticació)

2.5.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme o entitat de dret públic subscriptora del certificat, a la qual es troba vinculat l'empleat.
OU, Organization Unit	Unitat en l'organització	"Empleat públic amb pseudònim de nivell alt d'autenticació"
Pseudonym	Pseudònim Obligatori segons ETSI EN 319 412-2	Ex: NIP 111111111
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física, que la vincula amb l'Administració, organisme o entitat de dret públic subscriptora del certificat.
CN, Common Name	Informar amb el pseudònim de l'organisme	Title/PSEUDONIM + " - " + NIP + " - " + Organization (AUT) Ex: SUBINSPECTOR - NIP 11111111 - ORGANITZACIÓ DE PROVES (AUT)
C, Country	País	C = "ES"

2.5.2. Extensions

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la CA, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-calssuers Access Location: < URL de localització del certificat de la CA.>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Key Usage	Sí	Digital Signature
X509v3 Extended Key Usage	-	Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.4.1.2 <URI de la DPC> User Notice: "Certificat electrònic d'empleat públic amb pseudònim de nivell alt d'autenticació." <OID associat a certificat d'empleat públic amb pseudònim de nivell alt> 2.16.724.1.3.5.4.1 <OID de la política de certificació ETSI: NCP+> 0.4.0.2042.1.2
X509v3 Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuari en el domini Windows del posseïdor de claus 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 del DN> OID: 2.16.724.1.3.5.4.1.3 = <CIF de l'entitat subscriptora>

2.6. Perfil dels Certificats de signatura de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim signatura)

2.6.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme, o entitat de dret públic, a la qual es troba vinculat l'empleat.
OU, Organization Unit	Unitat en la organització	"Empleat públic amb pseudònim de nivell alt de signatura."
Pseudonym	Pseudònim Obligatori segons ETSI EN 319 412-2	Ex: NIP 111111111
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física, que la vincula amb l'administració, organisme o entitat de dret públic subscriptora del certificat.
CN, Common Name	Informar amb el pseudònim de l'organisme	Title/PSEUDONIM + " - " + NIP + " - " + Organization (SIG) Ex: SUBINSPECTOR - NIP 11111111 - ORGANITZACIÓ DE PROVES (SIG)
C, Country	País	C = "ES"

2.6.2. Extensions

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la CA, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-caIssuers Access Location: < URL de localització del certificat de la CA.>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la DPC corresponent> 1.3.6.1.4.1.15096.1.3.2.4.1.1 <URI de la DPC> User Notice: " Certificat qualificat de signatura de empleat públic amb pseudònim de nivell alt." <OID associat a certificat d'empleat públic amb pseudònim de nivell alt> 2.16.724.1.3.5.4.1 <OID de la política de certificació 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 anys 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	Sí	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 del DN> OID: 2.16.724.1.3.5.4.1.3 = <CIF de l'entitat subscriptora>

2.7. Perfil dels Certificats qualificats d'autenticació i signatura d'empleat públic amb pseudònim de nivell mig (T-CATP pseudònim)

2.7.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme, o entitat de dret públic, a la qual es troba vinculat l'empleat.
OU, Organization Unit	Unitat en la organització	"Empleat públic amb pseudònim de nivell mig."
Pseudonym	Pseudònim Obligatori segons ETSI EN 319 412-2	Ex: NIP 111111111
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física, que la vincula amb l'administració, organisme o entitat de dret públic subscriptora del certificat.
CN, Common Name	Informar amb el pseudònim de l'organisme	Title/PSEUDONIM + " - " + NIP + " - " + Organization (TCAT) Ex: SUBINSPECTOR - NIP 11111111 - ORGANITZACIÓ DE PROVES (TCAT)
C, Country	País	C = "ES"

2.7.2. Extensions

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la CA, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-calssuers Access Location: < URL de localització del certificat de la CA.>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la DPC corresponent> 1.3.6.1.4.1.15096.1.3.2.4.2 <URI de la DPC> User Notice: "Certificat qualificat empleat públic amb pseudònim de nivell mig" <OID associat a certificat d'empleat públic amb pseudònim de nivell mig/substancial> 2.16.724.1.3.5.4.2 <OID de la política de certificació 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 anys 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	Sí	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 del DN> OID: 2.16.724.1.3.5.4.2.3 = <CIF de l'entitat suscriptora>

2.8. Perfil dels Certificats d'autenticació i signatura de representant davant les Administracions Públiques (T-CAT representant)

2.8.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme o entitat de dret públic subscriptora del certificat a la qual representa el representant.
OU, Organization Unit	Unitat en l'organització	"Representant davant les AAPP de nivell alt"
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física, que la vincula amb l'Administració, organisme o entitat de dret públic subscriptora del certificat.
Serial Number	NIF	Número del document d'identitat de l'empleat públic amb la semàntica proposta per la norma ETSI EN 319 412-1 ⁵
SN, Surname	Cognoms (persona física)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI / Passaport, ...)
Given name	Nom	Nom, d'acord amb el document d'identitat (DNI / Passaport, ...)
CN, Common Name	Nom , cognoms i NIF	Veure taula específica. Exemple: "99949992L Nomdos Especimendos Especimendos (R: Q0000000J)"
C, Country	País	C = "ES"
Organization Identifier		Segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat, p.e. VATES- Q0000000J)
Description (2.5.4.13)	Dades de representació	Reg:XXX /Fulla:XXX /Tom:XXX /Secció:XXX /Llibre:XXX/ Foli:XXX /Data: dd-mm-aaaa /Inscripció:XXX Notari: Nomdos Especimendos Especimendos /Núm Protocol: XXX /Data Atorgament: dd-mm-aaaa En Butlletins o Diaris Oficials: Butlletí: XXX /Data: dd-mm-aaaa /Número resolució: XXX

⁵ SerialNumber = p. ex: IDCES-99949992L. 3 caràcters per indicar el tipus de document (IDC= document nacional d'identitat, PAS=passaport, ...) + 2 caràcters per identificar el país (ÉS) + Número d'identitat (Printable String)) Size [RFC 5280] 64

2.8.2. Common name

Camp	Contingut	Exemple	Grandària (*)
NIF	Número DNI/NIE	99949992L	10
Nom	D'acord amb el document d'identitat	Nomdos	
Cognom 1	D'acord amb el document d'identitat	Especimendos	
Literal	(R:		4
NIF de l'entitat representada	NIF de l'entitat representada, tal i com figura en els registres oficials	Q0000000J	9
Literal	)		2

(*) tenint en compte espai en blanc posterior

2.8.3. Extensions

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la EC, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-caIssuers Access Location: <URI del certificat de l'EC emissora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la política de certificació corresponent al certificat> 1.3.6.1.4.1.15096.1.3.2.8.1.1 <URI de la DPC> User Notice: "Certificat electrònic de representant davant les AAPP de nivell alt." <OID de certificat de representant de persona jurídica> 2.16.724.1.3.5.8 <OID de la política de certificació 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 anys 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	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	Client Authentication SmartCardLogon Adobe Authentic Documents Trust
X509v3 Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuari en el domini Windows del posseïdor de claus 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. Perfil dels Certificats de signatura de empleat públic de nivell alt (T-CAT signatura)

2.9.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme o entitat de dret públic subscriptora del certificat, a la qual es troba vinculat l'empleat.
OU, Organization Unit	Unitat en l'organització	"Empleat públic de nivell alt de signatura"
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física que la vincula amb l'administració, organisme o entitat de dret públic subscriptora del certificat.
Serial Number	NIF	Número el document d'identitat de l'empleat públic amb la semàntica proposta per la norma ETSI EN 319 412-1 ⁶
SN, Surname	Cognoms (persona física)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI / Passaport, ...)
Given name	Nom	Nom, d'acord amb document d'identitat (DNI, passaport, ...)
CN, Common Name	Nom, cognoms i NIF	Nom i dos cognoms d'acord amb document d'identitat (DNI / Passaport) + NIF de l'empleat públic + " (SIG)"
C, Country	País	C = "ES"
Organization Identifier		Segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat)

⁶ SerialNumber = p. ex: IDCES-99949992L. 3 caràcters per indicar el tipus de document (IDC= document nacional d'identitat, PAS=passaport, ...) + 2 caràcters per identificar el país (ÉS) + Nombre d'identitat (Printable String)) Size [RFC 5280] 64

2.9.2. Extensions

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la EC, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificat de l'EC emissora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys 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	Sí	Content Commitment
X509v3 Extended Key Usage	-	Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.7.1.1 <URI de la DPC> User Notice: " Certificat qualificat de signatura de empleat públic de nivell alt." <OID associat a certificat d'empleat públic de nivell alt> 2.16.724.1.3.5.7.1 <OID de la política de certificació 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 d'empleat públic de nivell alt " OID: 2.16.724.1.3.5.7.1.2 = <O del DN> OID: 2.16.724.1.3.5.7.1.3 = <CIF de l'entitat subscriptora> OID: 2.16.724.1.3.5.7.1.4 = <serialNumber del DN> OID: 2.16.724.1.3.5.7.1.6 = <Given name> OID: 2.16.724.1.3.5.7.1.7 = <Primer cognom de l'empleat públic> OID: 2.16.724.1.3.5.7.1.8 = <Segon cognom de l'empleat públic>

2.10. Perfil dels Certificats d'autenticació i signatura de treballador públic de nivell mitjà (T-CATP Treballador públic)

2.10.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme o entitat de dret públic subscriptora del certificat, a la qual es troba vinculat el treballador.
OU, Organization Unit	Unitat en l'organització	"Treballador públic de nivell mig"
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física que la vincula amb l'administració, organisme o entitat de dret públic subscriptora del certificat.
Serial Number	NIF	Número el document d'identitat del signant amb la semàntica proposta per la norma ETSI EN 319 412-1 ⁷
SN, Surname	Cognoms (persona física)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI / Passaport, ...)
Given name	Nom	Nom, d'acord amb document d'identitat (DNI, passaport, ...)
CN, Common Name	Nom, cognoms i NIF	Nom i dos cognoms d'acord amb document d'identitat (DNI / Passaport) + NIF del treballador públic + " (SIG)"
C, Country	País	C = "ES"
Organization Identifier		Segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat)

⁷ SerialNumber = p. ex: IDCES-99949992L. 3 caràcters per indicar el tipus de document (IDC= document nacional d'identitat, PAS=passaport, ...) + 2 caràcters per identificar el país (ÉS) + Nombre d'identitat (Printable String)) Size [RFC 5280] 64

2.10.2. Extensions

Extensió	Crític a	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la EC, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificat de l'EC emissora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage		Client Authentication Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.86.3 <URI de la DPC> <User Notice> "Certificat electrònic de treballador públic de nivell mig." <OID de la política de certificació 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 anys 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. Perfil dels Certificats d'autenticació i signatura de treballador públic de nivell alt (T-CAT Treballador públic)

2.11.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme o entitat de dret públic subscriptora del certificat, a la qual es troba vinculat el treballador.
OU, Organization Unit	Unitat en l'organització	"Treballador públic de nivell alt"
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física que la vincula amb l'administració, organisme o entitat de dret públic subscriptora del certificat.
Serial Number	NIF	Número el document d'identitat del signant amb la semàntica proposta per la norma ETSI EN 319 412-1 ⁸
SN, Surname	Cognoms (persona física)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI / Passaport, ...)
Given name	Nom	Nom, d'acord amb document d'identitat (DNI, passaport, ...)
CN, Common Name	Nom, cognoms i NIF	Nom i dos cognoms d'acord amb document d'identitat (DNI / Passaport) + NIF del treballador públic + " (TCAT)"
C, Country	País	C = "ES"
Organization Identifier		Segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat)

⁸ SerialNumber = p. ex: IDCES-99949992L. 3 caràcters per indicar el tipus de document (IDC= document nacional d'identitat, PAS=passaport, ...) + 2 caràcters per identificar el país (ÉS) + Nombre d'identitat (Printable String)) Size [RFC 5280] 64

2.11.2. Extensions

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la EC, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys 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	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	Client Authentication SmartCardLogon Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.82.2 <URI de la DPC> User Notice: "Certificat electrònic de treballador públic de nivell alt." <OID de la política de certificación ETSI: QCP-n-qscd> 0.4.0.194112.1.2
X509v3 Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuari en el domini Windows del posseïdor de claus 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. Descripció de Perfils de Certificats de Ciutadania

3.1. Perfil dels Certificats de Ciutadà (idCAT certificat)

3.1.1. Certificat

Camp del DN	Nom	Descripció
CN, Common Name	Nom	Cognoms i Nom del signant + “ - DNI “ + número del document d'identificació. Ex:Nomdos Especimendos Especimendos – DNI 99949992L
Serial Number	Número de sèrie	Número del document d'identitat del signatari, amb la semàntica proposta per la norma ETSI EN 319 412-1
SN, Surname	Cognoms	Cognoms del signatari tal com apareixen en el document d'identitat utilitzat
GN, givenName	Nom de pila	Nom de pila del signatari, tal com apareix en el document d'identitat utilitzat
C, Country	País	“País d'expedició del document identificatiu del subscriptor.”

3.1.2. Extensions dels certificats

Extensió	Crítica	Valor
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	TLS Web Client Authentication Adobe Authentic Documents Trust
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtinguda a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la CA, obtingut a partir del hash de la mateixa>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la política de certificació corresponent al certificat> 1.3.6.1.4.1.15096.1.3.2.86.2 <URI de la DPC> User Notice: "idCAT Certificat." <OID de la política de certificació ETSI: 0.4.0.194112.1.0> (Corresponent a la política per a certificats EU qualificats emesos a persones físiques "QCP-n", sense ús d'un DSCF)
qcStatements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys 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 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d' accés al servei OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificat de l'EC emissora>

4. Descripció dels Perfils de Certificats de Dispositius i Infraestructura

4.1. Perfil dels Certificats de Segell Electrònic Avançat (Segell nivell mig)

4.1.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Contindrà la denominació de l'Administració a la qual pertany l'organisme.
Organization Identifier		Identificador de la organizaci3n distinto del nombre seg3n la norma t3cnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
OU, Organization Unit	Unitat de l'organitzaci3n	"Certificat de segell electr3nic nivell mig"
Serial Number	CIF	CIF de l'Administraci3n P3blica, 3rgan o entitat de dret p3blic
SN, Surname (Opcional)	Cognoms (persona f3sica)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI o NIE-)
Given name (Opcional)	Nom (persona f3sica)	Nom, d'acord amb el document d'identitat (DNI, NIE) del responsable de la cust3dia de la clau privada
CN, Common Name	Denominaci3n del sistema o aplicaci3n	p.e. "PLATAFORMA DE VALIDACI3N DE L'AJUNTAMENT DE xxx"
C, Country	Pa3s	C= ES.

4.1.2. Extensions dels certificats

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	TLS Web Client Authentication Adobe Authentic Documents Trust
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtinguda a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la EC, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys 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. Extensions de nivell mitjà

Extensió	Crítica	Valors
X509v3 Certificate Policies	-	<OID de la política de certificació corresponent al certificat> 1.3.6.1.4.1.15096.1.3.2.6.2 <URI de la DPC> User Notice: "Certificat de segell electrònic nivell mig." <OID associat als certificats de segell de nivell mitjà / substancial> 2.16.724.1.3.5.6.2 <OID "for EU qualified certificates issued to legal persons" segons 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 del DN> OID: 2.16.724.1.3.5.6.2.3 = <serialNumber del DN> OID: 2.16.724.1.3.5.6.2.4 = <NIF/NIE del custodi> OID: 2.16.724.1.3.5.6.2.5 = <CN del DN> OID: 2.16.724.1.3.5.6.2.6 = <Given name> OID: 2.16.724.1.3.5.6.2.7 = <Primer cognom del custodi> (1) OID: 2.16.724.1.3.5.6.2.8 = <Segon cognom del custodi> (2) OID: 2.16.724.1.3.5.6.2.9 = <Correu electrònic del custodi>

1. D'acord amb document d'identitat (DNI, NIE)
2. D'acord amb document d'identitat (DNI, NIE)

4.2. Perfil dels Certificats d'Aplicació (Dispositiu aplicació)

4.2.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Contindrà la denominació de l'Administració a la qual pertany l'organisme
Organization Identifier		Identificador de l'organització diferent del nom segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat)
OU, Organization Unit	Unitat en l'organització	"Certificat d'aplicació"
Serial Number	CIF	CIF de l'Administració Pública, òrgan o entitat de dret públic
CN, Common Name	Denominació del sistema o aplicació	p.e. "PLATAFORMA DE VALIDACIÓ DE L'AJUNTAMENT DE xxx"
C, Country	País	C= ES.

4.2.2. Extensions dels certificats

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	TLS Web Client Authentication Adobe Authentic Documents Trust
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la CA, obtingut a partir del hash de la mateixa>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificat de l'EC emissora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys 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 de la política de certificació corresponent al certificat> 1.3.6.1.4.1.15096.1.3.2.91.1 <URI de la DPC> 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. Perfil dels Certificats de Segell de Temps Qualificats

4.3.1. Certificat

Camp del DN	Nom	Descripció
O, Organization	Organització	Consorti Administració Oberta de Catalunya
Organization Identifier		Identificador de l'organització diferent del nom segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat)
CN, Common Name	Nom	<i>CONSORCI AOC Q TSU + "any de l'emissió"</i>
C, Country	País	C = "ES"

4.3.2. Extensions dels certificats qualificats

Extensió	Crítica	Valors
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	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la CA, obtingut a partir del hash de la mateixa>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.112 <URI de la DPC> User Notice: "Certificat de Servei de Segell Qualificat de Temps" < OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-I> 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 anys 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 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-calssuers Access Location: < URL de localització del certificat de la CA.>
Private Key Usage Period		<Data inici de validesa i data final de validesa, màxim 2 anys>