Consorci
Administració Oberta
de Catalunya

Descripció dels perfils de Certificats Consorci AOC

Generalitat
de Catalunya

LOCALRET

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://www.aoc.cat/catcert/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

Índex

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 d'Hisenda i Funció Pública; 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://www.aoc.cat/catcert/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 publicación 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.

SN, Serial Number	NIF	Número del document d'identitat del signatari amb la semàntica proposta per la norma ETSI EN 319 412-1[1]
Surname	Cognoms (persona física)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI / Passaport, …) + ” - DNI” + NIF de l'empleat públic
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) + “ – DNI” + 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. ej: IDCES-00000000G. 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-caIssuers Access Location: <URI del certificat de l'EC emissora>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Sí	Digital Signature Key encipherment
X509v3 Extended Key Usage		Email protection 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 . Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <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 per SMIME) rfc822Name: mail de contacte (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 empleatpúblic 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.
SN, Serial Number	NIF	Número del document d'identitat del signatari, amb la semàntica proposta per la norma ETSI EN 319 412-1[2]
Surname	Cognoms (persona física)	Primer i segon cognom (d'acord amb el document d'identitat – DNI / Passaport, …) + " - DNI " + NIF de l'empleat públic
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) + " – DNI " + 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. ej: IDCES-00000000G. 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	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage		Email protection Client Authentication
X509v3 Certificate Policies	-	<OID 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. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <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 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1

X509v3 Subject Alternative Name	-	rfc822Name: mail de contacte (Opcional) 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.
SN, Serial Number	NIF	Número del document d'identitat del signatari, amb la semàntica proposta per la norma ETSI EN 319 412-1[3]
Surname	Cognoms (persona física)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI / Passaport, …) + " - DNI " + NIF de l'empleat públic.
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) + " – DNI " + 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. ej: IDCES-00000000G. 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'acces al servei OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificat de l' EC emissora>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication
X509v3 Certificate Policies	-	<OID 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. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <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 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Subject Alternative Name	-	rfc822Name: mail de contacte (Opcional)

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.
SN, Serial Number	NIF	NIF o NIE de l'empleat públic. Preferiblement s'aplicarà la semàntica proposta per la norma ETSI EN 319 412-1[4]
Surname	Cognoms (persona física)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI, Passaport, …)+" - DNI " + NIF de la persona vinculada
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) + " – DNI " + 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. ej: IDCES-00000000G. 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'acces al servei OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificat de l'EC emissora>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Sí	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.82.1 <URI de la DPC> User Notice: "Certificat electrònic de persona vinculada de nivell alt. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID de la política de certificació ETSI: QCP-n-qscd> 0.4.0.194112.1.2
X509v3 Subject Alternative Name	-	(opcional per SMIME) rfc822Name: mail de contacte (opcional) otherName-userPrincipalName (UPN): Usuari en el domini Windows del posseïdor de claus

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	Ej: 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	Pseudonym + “ - “ + Title + (AUT) Ex: NIP 11111111 - SUBINSPECTOR (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-caIssuers Access Location: < URL de localització del certificat de la CA.>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Sí	Digital Signature Key encipherment
X509v3 Extended Key Usage		Email Protection Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.4.1.2 <URI de la DPC> User Notice: "Certificat electrònic d'empleat públic amb pseudònim de nivell alt d'autenticació. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <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.”
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	Pseudonym + “ - “ + Title + (SIG) Ex: NIP 11111111 – SUBINSPECTOR (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-calssuers Access Location: < URL de localització del certificat de la CA.>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.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. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <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	Sí	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Content Commitment
X509v3 Extended Key Usage		Email protection
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.4.1.1 = "Certificat qualificat de signatura d'empleat públic amb pseudònim de nivell alt" OID: 2.16.724.1.3.5.4.1.2 = <O del DN> OID: 2.16.724.1.3.5.4.1.3 = <CIF de l'entitat suscriptora>

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

2.7.1. 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.
SN, 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]
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: "12345678Z Pedro Antonio López (R: B0085974Z)"
C, Country	País	C = "ES"
Organization Identifier		Segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat, p.e. VATES-B0085974Z)
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: Nom Cognom1 Cognom2 /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. ej: IDCES-00000000G. 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

2.7.2. Common name

Camp	Contingut	Exemple	Grandària(*)
NIF	Número DNI/NIE	12345678Z	10
Nom	D'acord amb el document d'identitat	Pedro Antonio	
Cognom 1	D'acord amb el document d'identitat	López	
Literal	(R:		4
NIF de l'entitat representada	NIF de l'entitat representada, tal i com figura en els registres oficials	Q0085974Z	9
Literal	)		2

(*) tenint en compte espai en blanc posterior

2.7.3. 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-calssuers Access Location: <URI del certificat de l'EC emissora>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.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. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <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	Sí	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1

X509v3 Key Usage	Sí	Digital Signature Content Commitment Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication SmartCardLogon
X509v3 Subject Alternative Name	-	(opcional per SMIME) rfc822Name: mail de contacto (opcional) otherName-userPrincipalName (UPN): Usuari en el domini Windows del posseïdor de claus

2.8. Perfil dels Certificats de signatura de empleat públic de nivell alt (T-CAT signatura)

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 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.
SN, 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]
Surname	Cognoms (persona física)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI / Passaport, …) + " - DNI " + NIF de l'empleat públic
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) + " – DNI " + 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-00000000G. 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

2.8.2. 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	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Sí	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Content Commitment
X509v3 Extended Key Usage	-	Email protection
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 . Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <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>

3. Descripció de Perfils de Certificats de Ciutadans

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: PEREZ MAS JOSE – DNI 123456789Z
serialNumber	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	"ES"

3.1.2. Extensions dels certificats

Extensió	Crítica	Valor
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Non Repudiation Key Encipherment
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection
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	-	http://epscd.catcert.net/crl/ec-sectorpublic.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. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A” <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: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d’ accés al servei OCSP> Access Method: Id-ad-caIssuers 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 organización distinto del nombre según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
OU, Organization Unit	Unitat de l'organització	"Certificat de segell electrònic nivell mig"
SN, Serial Number	CIF	CIF de l'Administració Pública, òrgan o entitat de dret públic
Surname (Opcional)	Cognoms (persona física)	Primer i segon cognoms (d'acord amb el document d'identitat – DNI o NIE-) + " - DNI " + NIF del custodi de la clau privada
Given name (Opcional)	Nom (persona física)	Nom, d'acord amb el document d'identitat (DNI, NIE) del responsable de la custòdia de la clau privada
CN, Common Name	Denominació del sistema o aplicació	p.e. "PLATAFORMA DE VALIDACIÓ DE L'AJUNTAMENT DE xxx"
C, Country	País	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	-	Email protection TLS Web Client Authentication
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-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Sí	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-eseal 0.4.0.1862.1.6.2

4.1.3. 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. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <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-l> 0.4.0.194112.1.1
X509v3 Subject Alternative Name	-	rfc822Name: mail de contacte 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 custodio> (1) OID: 2.16.724.1.3.5.6.2.8 = <Segon cognom del custodio> (2) OID: 2.16.724.1.3.5.6.2.9 = <correu electrònic del custodio>

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"
SN, 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	-	Email protection TLS Web Client Authentication
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	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Sí	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-eseal 0.4.0.1862.1.6.2
X509v3 Certificate Policies	-	<OID 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. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" < OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-l> 0.4.0.194112.1.1
X509v3 Subject Alternative Name	-	rfc822Name:mail de contacte (opcional)

4.3. Perfil dels Certificats de Seu Electrònica (Seu-e nivell mig)

4.3.1. Certificat

Camp del DN	Valor	Descripció
CN, Common Name	Nom	Denominació de nom de domini on residirà el certificat Ha de coincidir amb el qual es troba en l'extensió Subject Alternative Names
O, Organization	Raó Social	Denominació (nom "oficial" de l'organització) del subscriptor de serveis de certificació
OU, Organizational Unit	Unitat en l'organització	*"Certificat de seu electrònica nivell mig"*
OU, Organizational Unit	Unitat en l'organització	*El nom descriptiu de la seu*

SN, SerialNumber	CIF	*Contindrà el NIF de l'entitat responsable de la seu electrònica*
OrganizationIdentifier		Identificador de l'organització Segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat)
businessCategory	"Government Entity"	Business Category
C, Country	País	*C=ES*
jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	País	Subject Jurisdiction of Incorporation or Registration *C=ES*
L, Locality	Municipi	Ciutat
S, State or Province	Provincia	Provincia

4.3.2. Extensions dels certificats

Extensió	Crítica	Valors
X509v3 Authority Key Identifier	-	<id de la clau pública de la EC, obtingut a partir del hash de la mateixa>
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Key Usage	Sí	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	Autenticació TLS web Server
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl

X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-caIssuers Access Location: <URI del certificat de la EC emissora>
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.5.2 <URI de la DPC> User Notice: "Certificat de seu electrònica de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID associat als certificats de seu de nivell mitjà / substancial> 2.16.724.1.3.5.5.2 <OID ETSI QCP-w> 0.4.0.194112.1.4
Qualified Certificate Statements		Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-web 0.4.0.1862.1.6.3
X509v3 Subject Alternative Name	-	dNSName: nom de domini on residirà el certificat

4.4. Perfil dels Certificats de Servidor Segur (Dispositiu SSL)

4.4.1. Certificat

Camp del DN	Valor	Descripció
CN, Common Name	Nom	(BR. 7.1.4.2.2.a) Aquest domini ha de coincidir amb l'indicat (o amb un dels indicats) en el Subject Alt Names).
O, Organization	Raó Social	Denominació (nom "oficial" de l'organització) del subscriptor de serveis de certificació
OU, Organizational Unit (Opcional)	Unitat en la organització	*El nom descriptiu del departament*
OrganizationIdentifier		Identificador de l'organització Segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat)

L, Locality	Ciutat	(BR. 7.1.4.2.2.e) Indicació requerida en existir el camp Organization (O)
C, Country	País	Codi de país de dos dígits segons ISO 3166-1. Per defecte “ÉS”. (BR. 7.1.4.2.2.h) Indicació requerida en existir el camp Organization (O)

Les indicacions (BR.X) són requisits de la *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* del CA/Browser Forum, en la versió vigent al moment de la publicació d'aquest perfil.

4.4.2. Extensions dels certificats

Extensió	Crítica	Valors
X509v3 Subject Alternative Name	-	URL, nom de domini o identificació del dispositiu o servei posseïdor de les claus o de l'aplicació.
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	Server Authentication (1.3.6.1.5.5.7.3.1)
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 1: Id-ad-ocsp (1.3.6.1.5.5.7.48.1) Access Location 1: <URI de acceso al servicio OCSP> Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2) Access Location 2: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl

X509v3 Certificate Policies	-	<OID de la política de certificació corresponent al certificat> 1.3.6.1.4.1.15096.1.3.2.51.1 <URI de la CPS> User Notice: "Certificat de dispositiu SSL. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"
X509v3 Subject Alternative Name	-	dNSName: nom de domini on residirà el certificat

4.5. Perfil dels Certificats de Servidor Segur Extended Validation (Dispositiu SSL EV)

4.5.1. Certificat

Camp del DN	Valor	Descripció
CN, Common Name	Nom	(EVG 9.2.3) Nom d'un únic domini. (BR. 7.1.4.2.2.a) Aquest domini ha de coincidir amb l'indicat (o un dels indicats) en el Subject Alt Names).
O, Organization	Raó Social	Nom Oficial de l'Organització subscriptora del certificat
OU, Organizational Unit (Opcional)	Unitat en la organització	*El nom descriptiu del departament*
SN, SerialNumber	CIF	CIF de l'Organització subscriptora del certificat (EVG 9.2.6) Registration Number
OrganizationIdentifier		Identificador de l'organització Segons la norma tècnica ETSI EN 319 412-1 (VATES + NIF de l'entitat)
businessCategory	"Government Entity"	(EVG 9.2.4) Business Category
C, Country	País	Codi de país de dos dígits segons ISO 3166-1. Per defecte "ES".(EVG 9.2.7) Country (required) (BR. 7.1.4.2.2.h) Indicació requerida al existir el camp Organization (O)
L, Locality		(EVG 9.2.7) Address of Place of Business: City (required) (BR. 7.1.4.2.2.e) Indicación requerida al existir el campo Organization (O)

jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	País	(EVG 9.2.5) Subject Jurisdiction of Incorporation or Registration

Les indicacions (BR.X) són requisits de la *Baseline Requeriments Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* del CA/Browser Forum, en la versió vigent al moment de la publicació d'aquest perfil.

Les indicacions (EVG 9.2.X) són requisits específics per a certificats *Extended Validation* segons estableix el CA/Browser Forum a les *Guidelines For The Issuance And Management Of Extended Validation Certificates*, en la versió vigent al moment de la publicació d'aquest perfil.

4.5.2. Extensions dels certificats

Extensió	Crítica	Valors
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la CA, obtingut a partir del hash de la mateixa>
X509v3 Subject Key Identifier	-	<id de la clau pública del certificat, obtingut a partir del hash de la mateixa>
X509v3 Key Usage	Sí	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	Server Authentication (1.3.6.1.5.5.7.3.1)
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI d'accés al servei OCSP> Access Method: Id-ad-caIssuers Access Location: <URI del certificat de la EC emissora>
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.51.2 <URI de la DPC> User Notice: “Certificat de dispositiu SSL EV. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A” <OID ETSI QCP-w> 0.4.0.194112.1.4

Qualified Certificate Statements		Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-web 0.4.0.1862.1.6.3
X509v3 Subject Alternative Name	-	dNSName: nom de domini on residirà el certificat

4.6. Perfil dels Certificats de Segell Qualificat de Temps

4.6.1. Certificat

Camp del DN	Valor	Descripció
CN, Common Name	Nomb	*Ha de contenir un Identificador de TSU que ha d'identificar de manera única la TSU corresponent, incloent referència al client*
O, Organization	Organització	Consorci Administració Oberta de Catalunya
OI, Organization Identifier	Identificador d'Organització	"VATES-Q0801175A"
C, Country	País	C=ES

4.6.2. Extensions dels certificats

Extensió	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	digitalSignature contentCommitment
X509v3 Extended Key Usage	Sí	id-kp-timeStamping {1.3.6.1.5.5.7.3.8}
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	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl

X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.111 <URI de la PC>https://www.aoc.cat/catcert/regulacio userNotice: “Certificat de Servei Segur de TSA qualificada”
id-ce-privateKeyUsagePeriod 2.5.29.16		*Té per objectiu limitar la validesa de la clau privada: 3 anys*
Authority Information Access	-	accessMethod: Id-ad-calssuers accessLocation: <URI d'accés al certificat de la CA emissora> accessMethod: Id-ad-ocsp accessLocation: <URI d'accés al servei OCSP>

Els Tokens de Timestamp qualificats, haurien d'incloure una instància de l'extensió qcStatements, d'acord amb la sintaxi definida en IETF RFC 3739 [i.3], clàusula 3.2.6.

L'extensió hauria d'incloure una instància de "esi4-*qtstStatement-1" d'acord amb el definit en l'Annex B de la norma ETSI TS 319 422 .