Consorci
Administració Oberta
de Catalunya

Descripció del perfil de certificats d'EC-SectorPublic

Generalitat
de Catalunya

LOCALRET

Control documental

Estat formal	Elaborat per: Servei de Certificació Digital		Aprovat per: Direcció del Consorci AOC
Data de creació	09/05/2018		
Control de versions	**Versió:**	1.0	
	Data:	09/05/2018	
	Descripció:	Adaptació a eIDAS. Adaptació a CertiCA (DTIC de MINHAP).	
Nivell accés informació	Pública		
Títol	Descripció de perfils de certificats d'EC-SectorPublic		
Control de còpies	Només les còpies disponibles a la web del Consorci AOC a https://www.aoc.cat/CATCert/Regulacio garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.		
Drets d'autor	Aquesta obra està subjecta a una llicència Reconeixement-No comercial-Sense obres derivades 3.0 Espanya de Creative Commons. Per veure'n una còpia, visiteu https://creativecommons.org/licenses/by-nc-nd/3.0/es/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.		

Índex

PERFIL DELS CERTIFICATS CDA-1_SGNM

Certificat

Campo del DN	Nom	Descripció
O, Organization	Organització	Contindrà la denominació de l'Administració a la que pertany l'organisme
Organization Identifier		Identificador de l'organització distint del nom Segons la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
OU, Organization Unit	Unitat a 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 document d'identitat – DNI o NIE-) + " - DNI " + NIF del custodi de la clau privada
Given name (Opcional)	Nom (persona física)	Nom de pila, d'acord amb document d'identitat (DNI, NIE) del custodi de la clau privada
CN, Common Name	Denominació del sistema o aplicació	p.e. "PLATAFORMA DE VALIDACIÓN DE L'AJUNTAMENT DE xxx"
C, Country	País	C= ES.

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 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 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

Extensions de nivel mig

Extensión	Crítica	Valores
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 mig / substancial> 2.16.724.1.3.5.6.2 <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 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)

PERFIL DELS CERTIFICATS CDA-1

Certificat

Campo del DN	Nom	Descripció
O, Organization	Organització	Contindrà la denominació de l'Administració a la que pertany l'organisme
Organization Identifier		Identificador de l'organització distint del nom Segons la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
OU, Organization Unit	Unitat a 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 VALIDACIÓN DE L'AJUNTAMENT DE xxx"
C, Country	País	C= ES.

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 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 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)

PERFIL DELS CERTIFICATS CDS-1_SENM

Certificat

Camp del DN	Valor	Descripció
CN, Common Name	Nom	Denominació de nom de domini on residirá el certificat Ha de coincidir amb el que es troba a l'extensió Subject Alternative Names
O, Organization	Raó Social	Denominació (nom "oficial" de l'organització) del suscriptor de serveis de certificació
OU, Organizational Unit	Unitat a l'organització	*"Certificat de seu electrònica nivell mig"*
OU, Organizational Unit	Unitat a 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 técnica ETSI EN 319 412-1 (VATES + NIF de la 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

Extensions dels certificats

Extensió	Crítica	Valors
X509v3 Authority Key Identifier	-	<id de la clau pública 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	-	Autenticación 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 l'EC emisora>
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 mig / 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 anys 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

PERFIL DELS CERTIFICATS CDS-1

Certificat

Camp del DN	Valor	Descripció
CN, Common Name	Nom	(BR. 7.1.4.2.2.a) Aquest domini ha de coincidir amb el indicat (o amb un dels indicats) en el Subject Alt Names).
O, Organization	Raó Social	Denominació (nom "oficial" de l'organització) del suscriptor de serveis de certificació
OrganizationIdentifier		Identificador de l'organització Segons la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entitat)
L, Locality	Ciutat	(BR. 7.1.4.2.2.e) Indicació requerida al existir el camp Organization (O)
C, Country	País	Codi de país de dos dígits segons ISO 3166-1. Per defecte "ES". (BR. 7.1.4.2.2.h) Indicació requerida al existir el camp Organization (O)

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

Extensions dels certificats

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	URL, nom de domini o identificació del dispositiu o servei posseidor de les claus o de la aplicació. Per a certificats multidomini, la URL seguirà el format "*.domini.com" o la IP (aquesta indicació está prohibida per a certificats EV)
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, 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 1: Id-ad-ocsp (1.3.6.1.5.5.7.48.1) Access Location 1: <URI d'accés al servei OCSP> Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2) Access Location 2: <URI del certificat de l'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 ón residirà el certificat

PERFIL DELS CERTIFICATS CDSQ-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 el indicat (o amb un dels indicats) en el Subject Alt Names).
O, Organization	Raó Social	Nombre Oficial de l'Organització subscriptora del certificat
SN, SerialNumber	CIF	CIF de l'Organització subscriptora del certificat (EVG 9.2.6) Registration Number
OrganizationIdentifier		Identificador de l'organització Segons la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entitat)
businessCategory	"Government Entity"	(EVG 9.2.4) Business Category
C, Country	País	Codi de país de dos dígits segons ISO 3166-1. Per defecto "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) Indicació requerida al existir el camp 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 requeriments de la *Baseline Requeriments Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* del CA/Browser Forum, a la versió vigent en el moment de publicació d'aquest perfil.

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

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 l'EC emisora>
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 anys 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 ón residirà el certificat

PERFIL DELS CERTIFICATS CPI-1

Certificat

Campo del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme o entitat de dret públic subscriptora del certificat, a la que es troba vinculat l'empleat.
OU, Organization Unit	Unitat a l'organització	"Treballador públic de nivell alt d'autenticació"
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física, que el vincula amb l'administració, organisme o entitat de dret públic subscriptora del certificat.
SN, Serial Number	NIF	Número del document d'identitat del signant, amb la semàntica proposada 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 de pila, d'acord amb document ' identitat (DNI, pasaport, ...)
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 + " (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=passaport, ...) + 2 caràcters per identificar el país (ES) + Número d'identitat (Printable String)) Size [RFC 5280] 64

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 emisora>
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 de treballador 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 de treballador 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 de l'empleat públic> OID: 2.16.724.1.3.5.7.1.8 = <Segon cognom de l'empleat públic>

PERFIL DELS CERTIFICATS CPISA-1

Certificat

Campo del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organismo o ens de dret públic subscriptora del certificat, a la que es troba vinculat l'empleat.
OU, Organization Unit	Unitat a l'organització	"Treballador públic de nivell mig"
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física, que el vincula amb l'administració, organismo o ens de dret públic subscriptora del certificat.
SN, Serial Number	NIF	Número del document d'identitat del signant, amb la semàntica proposada per la norma ETSI EN 319 412-1[2]
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 de pila, 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 + " (TCAT")"
C, Country	País	C = "ES"
Organization Identifier		Segons la norma técnica 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 (ES) + Número d'identitat (Printable String)) Size [RFC 5280] 64

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 emisora>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage		Email protection Client Authentication
X509v3 Certificate Policies	-	<OID 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 treballador públic de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID que indica certificat de empleat públic de nivell mig> 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: 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 de treballador públic de nivell mig 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>

PERFIL DELS CERTIFICATS CPISA-2

Certificat

Campo del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme o ens de dret públic subscriptora del certificat, a la que es troba vinculat l'empleat.
OU, Organization Unit	Unitat a l'organització	"Persona vinculada de nivell mig"
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física, que el vincula amb l'administració, organisme o ens de dret públic subscriptora del certificat.
SN, Serial Number	NIF	Número del document d'identitat del signant, amb la semàntica proposada 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 de pila, 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 + " (TCAT")"
C, Country	País	C = "ES"
Organization Identifier		Segons la norma técnica 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 (ES) + Número d'identitat (Printable String)) Size [RFC 5280] 64

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 emisora>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication
X509v3 Certificate Policies	-	<OID 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 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 Subject Alternative Name	-	rfc822Name: mail de contacte (Opcional)

PERFIL DELS CERTIFICATS CPISQ-2

Certificat

Campo del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organismo o entitat de dret públic subscriptora del certificat, a la que 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 el 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 proposada 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 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 la persona vinculada + " (TCAT)"
C, Country	País	C = "ES"
Organization Identifier		Segons la norma técnica 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 (ES) + Número d'identitat (Printable String)) Size [RFC 5280] 64

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 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 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

PERFIL DELS CERTIFICATS CPPI-1

Certificat

Campo del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organisme o entitat de dret públic subscriptora del certificat, a la que es troba vinculat l'empleat.
OU, Organization Unit	Unitat a l'organització	"Treballador públic amb pseudònim de nivell alt d'autenticació"
Pseudonym	Pseudònim Obligatori segons ETSI EN 319 412-2	Ex: NIP 111111111
CN, Common Name	Cal informar el pseudònim i l'organisme	Pseudonym + " - " + Title + (AUT) Ex: NIP 11111111 - SUBINSPECTOR (AUT)
C, Country	País	C = "ES"

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 de treballador 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 public 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[5]
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 de treballador 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>

5

PERFIL DELS CERTIFICATS CPPSQ-1

Certificat

Campo del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organismo o ens de dret públic subscriptora del certificat, a la que es troba vinculat l'empleat.
OU, Organization Unit	Unitat a l'organització	"Treballador públic amb pseudònim de nivell alt."
Pseudonym	Pseudònim Obligatori segons ETSI EN 319 412-2	Ex: NIP 111111111
CN, Common Name	Cal informar el pseudònim i l'organisme	Pseudonym + " - " + Title + (SIG) Ex: NIP 11111111 – SUBINSPECTOR (SIG)
C, Country	País	C = "ES"

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 treballador públic amb pseudònim de nivell alt. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID associat a certificat d'empleat public 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 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 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.4.1.1 = "Certificat qualificat de signatura de treballador 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 la entitat subscriptora>

PERFIL DELS CERTIFICATS CPRISQ-1

Certificat

Campo del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organismo o entitat de dret públic subscriptora del certificat, a la que representa el representant.
OU, Organization Unit	Unitat a l'organització	"Representant davant les AAPP de nivell alt"
SN, Serial Number	NIF	Número del document d'identitat de l'empleat públic amb la semàntica proposada 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, …)
Given name	Nom	Nom de pila, d'acord amb 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 técnica 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 Otorgament: dd-mm-aaaa En Butlletins o Diaris Oficials: Butlletí: XXX /Data: dd-mm-aaaa /Número resolució: XXX

Common name

Camp	Contingut	Exemple	Tamany(*)
NIF	Número DNI/NIE	12345678Z	10

[6] 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 (ES) + Número d'identitat (Printable String)) Size [RFC 5280] 64

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'ens representat	NIF de l'ens reprentat, tal i com figura amb els registres oficials	Q0085974Z	9
Literal	)		2

(*) comptant espai en blanc posterior

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 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> 1.3.6.1.4.1.15096.1.3.2.8.1.1 <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 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	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 contacte (opcional) otherName-userPrincipalName (UPN): Usuari en el domini Windows del posseïdor de claus

PERFIL DELS CERTIFICATS CPSQ-1

Certificat

Campo del DN	Nom	Descripció
O, Organization	Organització	Denominació (nom "oficial") de l'Administració, organismo o entitat de dret públic subscriptora del certificat, a la que es troba vinculat l'empleat.
OU, Organization Unit	Unitat a l'organització	"Treballador públic de nivell alt de signatura"
Title (opcional)	Càrrec	Ha d'incloure el càrrec de la persona física, que el 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 proposada per la norma ETSI EN 319 412-1[7]
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 de pila, 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 técnica ETSI EN 319 412-1 (VATES + NIF de l' entitat)

[7] 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 (ES) + Número d'identitat (Printable String)) Size [RFC 5280] 64

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 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 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 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 treballador 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 de treballador 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>