Consorci
Administració Oberta
de Catalunya

Description of certificate profiles issued by EC-SectorPublic

Generalitat
de Catalunya

LOCALRET

Document control

Formal status	Created by: Digital Certification Service	Approved by: Consorci AOC General Direction
Creation date	09/05/2018	
Version control	**Version:**	1.0
	Date:	09/05/2018
	Description:	eIDAS adaptation. CertiCA adaptation (DTIC of MINHAP).
Access level information	Public	
Título	Description of certificate profiles issued by EC-SectorPublic	
Copies control	Only the versions available on the website of the Consorci AOC in https://www.aoc.cat/CATCert/Regulacio are guaranteed complete and updated. All hard copy or electronic copies printed or stored in different locations will be considered uncontrolled copies.	
Rights of authorship	This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Spain of Creative Commons. To see a copy, visit https://creativecommons.org/licenses/by-nc-nd/3.0/es/deed.ca or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.	

Índex

PROFILE OF CDA-1_SGNM CERTIFICATES

Certificate

DN field	Name	Description
O, Organization	Organization	Shall contain the administration name to which the body pertains
Organization Identifier		Identifier of the Organization (different from name) according to the technical standard ETSI EN 412-1 319 (VATES + identification number of the entity)
OU, Organization Unit	Organization unit hierarchy within a domain	"Certificat de segell electrònic nivell mig"
SN, Serial Number	CIF (in Spain)	IDENTIFICATION NUMBER of the public administration, organ or entity of public law
Surname (Optional)	Surname (physical person)	First and second surname (as it appears on formal identification document - National Id Document or National Id for Foreigners) + "-DNI" +VAT number of the private key owner
Given name (optional)	Name (of physical person)	First name as it appears on formal identification document (National Id Document, National Id for Foreigners) of the private key owner
CN, Common Name	Name of system or application	e.g. "PLATAFORMA DE VALIDACIÓN DE L'AJUNTAMENT DE xxx"
C, Country	Country	C= ES

Certificate extensions

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

Mid-level extensions

extension	Critical	Values
X509v3 Certificate Policies	-	< OID of the Certification policy corresponding to the certificate > 1.3.6.1.4.1.15096.1.3.2.6.2 < URI of the DPC > User Notice: "Certificat de segell electrònic nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID associated with stamp certificates of mid/substantial level> 2.16.724.1.3.5.6.2 < OID "for EU qualified certificates issued to legal persons" according to ETSI in 319 411-2: QCP-the > 0.4.0.194112.1.1
X509v3 Subject Alternative Name	-	rfc822Name: Contact mail address directoryName: OID: 2.16.724.1.3.5.6.2.1 = "Certificat de segell electrònic nivell mig" OID: 2.16.724.1.3.5.6.2.2 = <O of DN> OID: 2.16.724.1.3.5.6.2.3 = <serialNumber of DN> OID: 2.16.724.1.3.5.6.2.4 = <Custodian VAT number/National Id for Foreigners> OID: 2.16.724.1.3.5.6.2.5 = <CN of DN> OID: 2.16.724.1.3.5.6.2.6 = <Given name> OID: 2.16.724.1.3.5.6.2.7 = <Custodian first surname> (1) OID: 2.16.724.1.3.5.6.2.8 = <Custodian second surname> (2) OID: 2.16.724.1.3.5.6.2.9 = <Custodian email address>

(1) In accordance with identification document (National Id Document, National Id for Foreigners)
(2) In accordance with identification document (National Id Document, National Id for Foreigners)

PROFILE OF CDA-1 CERTIFICATES

Certificate

DN field	Name	Description
O, Organization	Organization	Shall contain the Administration name to which the body pertains
Organization Identifier		Identifier of the Organization (different from name) according to the technical standard ETSI EN 412-1 319 (VATES + VAT number of the entity)
OU, Organization Unit	Organization unit hierarchy within the domain (DN)	"Certificat d'aplicació"
SN, Serial Number	CIF (ES)	IDENTIFICATION NUMBER of the public administration, organ or entity of public law
CN, Common Name	Name of system or application	e.g.. "PLATAFORMA DE VALIDACIÓN DE L'AJUNTAMENT DE xxx"
C, Country	Country	e.g. C= ES.

Certificate extensions

extension	Critical	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Key Usage	Yes	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	Email protection TLS Web Client Authentication
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	< id of the CA certificate public key, obtained from the hash of the public key in question>

X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: < URI to access the OCSP service > Access Method: Id-ad-caIssuers Access Location: < URI of the certificate of the issuer EC>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Yes	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-eseal 0.4.0.1862.1.6.2
X509v3 Certificate Policies	-	<OID of the Certification policy corresponding to the certificate > 1.3.6.1.4.1.15096.1.3.2.91.1 < URI of the DPC > User Notice: "Certificat d'aplicació. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" < OID "for EU qualified certificates issued to legal persons" according to ETSI in 319 411-2: QCP-the > 0.4.0.194112.1.1
X509v3 Subject Alternative Name	-	rfc822Name: Contact mail (optional)

PROFILE OF CDS-1_SENM CERTIFICATES

Certificate

DN field	Value	Description
CN, Common Name	Name	Domain name where the certificate will reside Value must match what is contained within the extension Subject Alternative Names
O, Organization	Company name	Certification services subscriber name (official name of the Organization)
OU, Organizational Unit	Unit of Organization	*"Certificat de seu electrònica nivell mig"*
OU, Organizational Unit	Unit of Organization	*Descriptive name of the Electronic Office*
SN, SerialNumber	CIF	*Shall contain the VAT number of the electronic officeresponsible entity*
OrganizationIdentifier		Identifier of the organization In accordance with the technical rules ETSI EN 319 412-1 (VATES + VAT number of the entity)
businessCategory	"Government Entity"	Business Category
C, Country	Country	*C=ES*
jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	Country	Country where the subject is incorporated or registered *C=ES*
L, Locality	Municipality	City
S, State or Province	Province	Province

Certificate extensions

extension	Critical	Values
X509v3 Authority Key Identifier	-	<id of the CA public key, obtained from the hash of the public key in question>
X509v3 Subject Key Identifier	-	< id of the certificate public key, obtained from the hash of the public key in question>

X509v3 Key Usage	Yes	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	TLS web server authentication
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: < URI to access the OCSP service > Access Method: Id-ad-caIssuers Access Location: < URI of the certificate of the issuer EC>
X509v3 Certificate Policies	-	<OID associated with the DPC> 1.3.6.1.4.1.15096.1.3.2.5.2 <URI of the DPC> User Notice: "Certificat de seu electrònica de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID associated with mid/substantial level electronic office certificates > 2.16.724.1.3.5.5.2 <OID ETSI QCP-w> 0.4.0.194112.1.4
Qualified Certificate Statements		Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-web 0.4.0.1862.1.6.3
X509v3 Subject Alternative Name	-	dNSName: domain name where the certificate shall reside

PROFILE OF CDS-1 CERTIFICATES

Certificate

DN field	Value	Description
CN, Common Name	Name	(BR. 7.1.4.2.2.a) This domain must match that indicated (or one of those listed) in the Subject Alt Names field).
O, Organization	Company name	Certification services subscriber name (official name of the Organization)
OrganizationIdentifier		Identifier of the Organization In accordance with the technical rules ETSI EN 319 412-1 (VATES + VAT number of the entity)
L, Locality	City	(BR. 7.1.4.2.2.e) Required due to the existence of the Organization (O) field.
C, Country	Country	defined 2-digit code for the country according to ISO 3166-1. By default "ES". (BR. 7.1.4.2.2.h) Required due to the existence of the Organization (O) field.

The indications (BR. X) are requirements of the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* of the CA/Browser Forum, in the version in force at the time of publication of this profile.

Certificate extensions

extension	Critical	Values
X509v3 Subject Alternative Name	-	URL, domain name or identification of the device or owner service of the keys or the application. For multi-domain certificates, the URL will follow the format "*.domini.com" or IP (this indication is prohibited for EV certificates)
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Key Usage	Yes	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	Server Authentication (1.3.6.1.5.5.7.3.1)

X509v3 Subject Key Identifier	-	<public key id of the certificate, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	<public key id of the CA certificate, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: < URI to access the OCSP service > Access Method: Id-ad-caissuers (1.3.6.1.5.5.7.48.2) Access Location: < URI of the certificate of the issuer EC >
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Certificate Policies	-	< OID of the Certification policy corresponding to the certificate > 1.3.6.1.4.1.15096.1.3.2.51.1 <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: domain name where the certificate will reside

PROFILE OF CDSQ-1 CERTIFICATES

Certificate

DN field	Value	Description
CN, Common Name	Name	(EVG 9.2.3) Unique domain name. (BR. 7.1.4.2.2.a)This domain must match that indicated (or one of those listed) in the Subject Alt Names field.
O, Organization	Company name	Official name of the certificate subscriber Organization
SN, SerialNumber	CIF	CIF of the certificate subscriber Organization (EVG 9.2.6) Registration Number
OrganizationIdentifier		Organization identifier According to technical standard ETSI EN 319 412-1 (VATES + VAT number of the entity)
businessCategory	"Government Entity"	(EVG 9.2.4) Business Category
C, Country	Country	defined 2-digit code for the country according to ISO ISO 3166-1. By default "ES".(EVG 9.2.7) Country (required) (BR. 7.1.4.2.2.h) Required due to the existence of the Organization (O) field.
L, Locality		(EVG 9.2.7) Address of Place of Business: City (required) (BR. 7.1.4.2.2.e) Required due to the existence of the Organization (O) field.
jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	Country	(EVG 9.2.5) Subject Jurisdiction of Incorporation or Registration

The indications (BR. X) are requirements of the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* of the CA/Browser Forum, in the version in force at the time of publication of this profile.

The indications (EVG 9.2. X) are specific requirements for *Extended Validation* certificates in accordance with the provisions of the CA/Browser Forum on the *Guidelines For The Issuance And Management Of Extended Validation Certificates*, in the version in force at the time of publication of this profile.

Certificate extensions

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

PROFILE OF CPI-1 CERTIFICATES

Certificate

DN field	Name	Description
O, Organization	Organization	"Official" name of the certificate subscriber Organization, body or entity of public law, to which the employee is associated
OU, Organization Unit	Organization Unit	“Treballador públic de nivell alt d'autenticació”
Title (optional)	Role, position	Should include the physical person position. That position associates the person with the certificate subscriber administration, body of entity of public law.
SN, Serial Number	National Id Number	Identification document number of the signing person, in accordance with the semantics proposed by the standard ETSI EN 319 412-1[1]
Surname	Surname (physical person)	First and second surnames as displayed on identification document (National Id Document / Passport, …) + ” - DNI” + VAT number of the public servant
Given name	First Name	First name as displayed on identification document (National Id Document / Passport, …)
CN, Common Name	First name, surnames and NIF	First name and two surnames as displayed on identification document (National Id Document/ Passport, …) + ” - DNI” + VAT number of the public servant “(AUT)”
C, Country	Country	C = “ES”
Organization Identifier		Following the technical standard ETSI EN 319 412-1 (VATES + VAT number of the entity)

[1]SerialNumber = e.g.: IDCES-00000000G. 3 characters to indicate the type of document (IDC = national identity document, PAS = passport, etc.) + 2 characters to identify the country (ES) + Identity Number (Printable String)) Size [RFC 5280] 64

Certificate extensions

extension	Critical	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Subject Key Identifier	-	<public key id of the certificate, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	<public key id of the CA certificate, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: < URI to access the OCSP service > Access Method: Id-ad-caIssuers Access Location: < URI of the certificate of the issuer EC >
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Yes	Digital Signature Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associated with the DPC> 1: 1.3.6.1.4.1.15096.1.3.2.7.1.2 <URI of the DPC> <User Notice> " Certificat electrònic de treballador públic de nivell alt d'autenticació . Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID of the policy of high level certification for public servant > 2.16.724.1.3.5.7.1 <OID of the certification policy ETSI: NCP+> 0.4.0.2042.1.2
X509v3 Subject Alternative Name	-	(optional per SMIME) rfc822Name: contact mail (optional) otherName-userPrincipalName (UPN): Windows domain user of the key holder directoryName: OID: 2.16.724.1.3.5.7.1.1 = "Certificat electrònic de treballador públic de nivell alt d'autenticació" OID: 2.16.724.1.3.5.7.1.2 = <O of DN> OID: 2.16.724.1.3.5.7.1.3 = <CIF of subscriber entity> OID: 2.16.724.1.3.5.7.1.4 = <serialNumber of DN> OID: 2.16.724.1.3.5.7.1.6 = <Given name> OID: 2.16.724.1.3.5.7.1.7 = <First surname of the public servant> OID: 2.16.724.1.3.5.7.1.8 = <Second surname of the public servant>

PROFILE OF CPISA-1 CERTIFICATES

Certificate

DN field	Name	Description
O, Organization	Organization	"Official" name of the certificate subscriber Organization, body or entity of public law, to which the employee is associated
OU, Organization Unit	Organization Unit	“Treballador públic de nivell mig”
Title (optional)	Role, position	Should include the physical person position. That position associates the person with the certificate subscriber administration, body of entity of public law.
SN, Serial Number	e.g. NIF	Identification document of the signing person, in accordance with the standard ETSI EN 319 412-1[2]
Surname	Surname (physical person)	First and second surnames as displayed on identification document (National Id Document / Passport, …) + ” - DNI” + VAT number of the public servant
Given name	First Name	First name as displayed on identification document (National Id Document / Passport, …)
CN, Common Name	First name, surnames and NIF	First name and two surnames as displayed on identification document (National Id Document / Passport, …) + ” - DNI” + VAT number of the public servant + “(TCAT”)”
C, Country	Country	C = “ES”
Organization Identifier		Following the technical standard ETSI EN 319 412-1 (VATES + VAT number of the entity)

[2]SerialNumber = e.g.: IDCES-00000000G. 3 characters to indicate the type of document (IDC = national identity document, PÂS= passport, etc.) + 2 characters to identify the country (ES) + Identity Number (Printable String)) Size [RFC 5280] 64

Extensions

extension	Critical	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Subject Key Identifier	-	<public key id of the certificate, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	<public key id of the CA certificate, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: < URI to access the OCSP service > Access Method: Id-ad-caIssuers Access Location: < URI of the certificate of the issuer EC >
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Yes	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage		Email protection Client Authentication
X509v3 Certificate Policies	-	<OID of the DPC> 1: 1.3.6.1.4.1.15096.1.3.2.7.3.1 <URI of the DPC> <User Notice> Certificat electrònic de treballador públic de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID which indicates mid-level certificate for public servant> 2.16.724.1.3.5.7.2 <OID of the certification policy ETSI: QCP-n> 0.4.0.194112.1.0
Qualified Certificate Statements		Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1

X509v3 Subject Alternative Name	-	rfc822Name: contact mail (optional) directoryName: OID: 2.16.724.1.3.5.7.2.1 = Mid-level electronic certificate for public servant OID: 2.16.724.1.3.5.7.2.2 = <O of DN> OID: 2.16.724.1.3.5.7.2.3 = <CIF of the subscriber entity> OID: 2.16.724.1.3.5.7.2.4 = <serialNumber ofl DN> OID: 2.16.724.1.3.5.7.2.6 = <Given name> OID: 2.16.724.1.3.5.7.2.7 = <First surname of the public servant> OID: 2.16.724.1.3.5.7.2.8 = <Second surname of the public servant> OID: 2.16.724.1.3.5.7.2.9 = <Email address of the public servant>

PROFILE OF CPISA-2 CERTIFICATES

Certificate

DN field	Name	Description
O, Organization	Organization	"Official" name of the certificate subscriber Organization, body or entity of public law, to which the employee is associated.
OU, Organization Unit	Organization Unit	"Persona vinculada de nivell mig"
Title (optional)	Role/Position	Should include the physical person position. That position associates the person with the certificate subscriber administration, body of entity of public law.
SN, Serial Number	NIF	Identification document number of the signer, in accordance with the semantics proposed by the standard ETSI EN 319 412-1[3]
Surname	Surnames (physical person)	First and second surnames (in accordance with document of identity (National Id Document / Passport, …) + " - DNI " + VAT number of public servant
Given name	First Name	First name, in accordance with document of identity (National Id Document / Passport, …)
CN, Common Name	First name, surnames and identity (NIF)	First name and two surnames as displayed on identification document (National Id Document / Passport, …) + " - DNI" + VAT number of the public servant+ " (TCAT")"
C, Country	Country	C = "ES"
Organization Identifier		Following the technical standard ETSI EN 319 412-1 (VATES + VAT number of the entity)

[3] SerialNumber = e.g.: IDCES-00000000G. 3 characters to indicate the type of document (IDC = national identity document, PAS= passport, etc.) + 2 characters to identify the country (ES) + Identity Number (Printable String)) Size [RFC 5280] 64

Extensions

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

PROFILE OF CPISQ-2 CERTIFICATES

Certificate

DN field	Name	Description
O, Organization	Organization	"Official" name of the certificate subscriber Organization, body or entity of public law, to which the employee is associated.
OU, Organization Unit	Organization Unit	“Persona vinculada de nivell alt”
Title (optional)	Role/position	Should include the physical person position. That position associates the person with the certificate subscriber administration, body of entity of public law.
SN, Serial Number	NIF	VAT number or National Id for Foreigners of public servant. Preferably in accordance with the semantics proposed by standard ETSI EN 319 412-1[4]
Surname	Surnames (physical person)	First and second surnames (in accordance with document of identity (National Id Document / Passport, …) + ” - DNI ” + VAT number of affiliated person
Given name	First name	First name, in accordance with document of identity (National Id Document / Passport, …)
CN, Common Name	First name, surnames and identity (NIF)	First name and two surnames as displayed on identification document (National Id Document / Passport, …) + ” - DNI” + VAT number of the affiliated person + “ (TCAT”)”
C, Country	Country	C = “ES”
Organization Identifier		Following the technical standard ETSI EN 319 412-1 (VATES + VAT number of the entity)

[4] SerialNumber = e.g: IDCES-00000000G. 3 characters to indicate the type of document (IDC = national identity document) + 2 characters to identify the country (ES) + Identity Number (Printable String)) Size [RFC 5280] 64

Extensions

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

PROFILE OF CPPI-1 CERTIFICATES

Certificate

DN field	Name	Description
O, Organization	Organization	"Official" name of the certificate subscriber Organization, body or entity of public law, to which the employee is associated
OU, Organization Unit	Organization Unit	“Treballador públic amb pseudònim de nivell alt d'autenticació”
Pseudonym	Mandatory Pseudonym in accordance with standard ETSI EN 319 412-2	Ex: NIP 111111111
CN, Common Name	It is necessary to provide pseudonym and body	Pseudonym + “ - “ + Title + (AUT) Ex: NIP 11111111 - SUBINSPECTOR (AUT)
C, Country	País	C = “ES”

Extensions

extension	Critical	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Subject Key Identifier	-	<public key id of the certificate, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	<public key id of the CA certificate, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: < URI to access the OCSP service > Access Method: Id-ad-caIssuers Access Location: < URI of the certificate of the issuer EC >
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Yes	Digital Signature Key encipherment
X509v3 Extended Key Usage		Email Protection Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associated with the DPC> 1.3.6.1.4.1.15096.1.3.2.4.1.2 <URI of the 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 associated with high-level certificate for public servant with pseudonym> 2.16.724.1.3.5.4.1 <OID of the certification policy ETSI: NCP+> 0.4.0.2042.1.2[5]
X509v3 Subject Alternative Name	-	(optional) otherName-userPrincipalName (UPN): Windows domain user of the key holder 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 of DN> OID: 2.16.724.1.3.5.4.1.3 = <CIF of subscriber entity>

5

PROFILE OF CPPSQ-1 CERTIFICATES

Certificate

DN field	Name	Description
O, Organization	Organization	"Official" name of the certificate subscriber Organization, body or entity of public law, to which the employee is associated.
OU, Organization Unit	Organization Unit	“Treballador públic amb pseudònim de nivell alt.”
Pseudonym	Mandatory Pseudonym in accordance with standard ETSI EN 319 412-2	Ex: NIP 111111111
CN, Common Name	It is necessary to provide pseudonym and body	Pseudonym + “ - “ + Title + (SIG) Ex: NIP 11111111 – SUBINSPECTOR (SIG)
C, Country	Country	C = “ES”

Extensions

extension	Critical	Values
X509v3 Basic Constraints	Yes	CA:FALSE
X509v3 Subject Key Identifier	-	<public key id of the certificate, obtained from the hash of the public key in question>
X509v3 Authority Key Identifier	-	<public key id of the CA certificate, obtained from the hash of the public key in question>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: < URI to access the OCSP service > Access Method: Id-ad-caIssuers Access Location: < URI of the certificate of the issuer EC >
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Certificate Policies	-	<OID of the corresponding DPC> 1.3.6.1.4.1.15096.1.3.2.4.1.1 <URI of the 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 associated with high-level certificate for public servant with pseudonym> 2.16.724.1.3.5.4. <OID of the certification policy ETSI: QCP-n-qscd> 0.4.0.194112.1.2
Qualified Certificate Statements	Yes	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 years Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Yes	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 of DN> OID: 2.16.724.1.3.5.4.1.3 = <CIF of subscriber entity >

PROFILE OF CPRISQ-1 CERTIFICATES

Certificate

DN field	Name	Description
O, Organization	Organization	"Official" name of the certificate subscriber Organization, body or entity of public law, to which the employee is associated.
OU, Organization Unit	Organization Unit	"Representant davant les AAPP de nivell alt"
SN, Serial Number	Identification (NIF)	Identification document number of public servant with the semantics proposed by the standard ETSI EN 319 412-1[6]
Surname	Surnames (physical person)	First and second surnames (in accordance with document of identity (National Id Document / Passport, …) + " - DNI " + VAT number of affiliated person
Given name	First name	First name, in accordance with document of identity (National Id Document / Passport, …)
CN, Common Name	First name, surnames and identity (NIF)	See specific table Example: "12345678Z Pedro Antonio López (R: B0085974Z)"
C, Country	Country	C = "ES"
Organization Identifier		Following the technical standard ETSI EN 319 412-1 (VATES + VAT number of the entity, e.g. VATES-B0085974Z)
Description (2.5.4.13)	Representation data	Reg:XXX /Page:XXX /Volume:XXX /Section:XXX /Book:XXX/ Sheet:XXX /Data: dd-mm-aaaa /Registration:XXX Notary: Name Surname1 Surname2/Protocol number: XXX /Grant Date: dd-mm-aaaa In Bulletins or Official Journals: Bulletin: XXX /Date: dd-mm-aaaa /Resolution Number: XXX

Common name

Field	Content	Example	Size(*)

[6] SerialNumber = e.g.: IDCES-00000000G. 3 characters to indicate the type of document (IDC = national identity document, PAS= passport, etc.) + 2 characters to identify the country (ES) + Identity Number (Printable String)) Size [RFC 5280] 64

NIF	Identification number (National Id Document/National Id for Foreigners)	12345678Z	10
Name	According to identification document	Pedro Antonio	
Surname 1	According to identification document	López	
Literal	(R:		4
NIF of the represented entity	VAT number of the represented entity, according to the official records	Q0085974Z	9
Literal	)		2

(*) counting blank spaces afterwards

extensions

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

X509v3 Subject Alternative Name	-	(optional for SMIME) rfc822Name: contact mail (optional) otherName-userPrincipalName (UPN): Windows domain user of the key holder

PROFILE OF CPSQ-1 CERTIFICATES

Certificate

DN field	Name	Description
O, Organization	Organization	"Official" name of the certificate subscriber Organization, body or entity of public law, to which the employee is associated.
OU, Organization Unit	Organization Unit	"Treballador públic de nivell alt de signatura"
Title (optional)	Role/position	Should include the physical person position. That position associates the person with the certificate subscriber administration, body of entity of public law.
SN, Serial Number	Identification (NIF)	Identification document number of public servant with the semantics proposed by the standard ETSI EN 319 412-1[7]
Surname	Surnames (physical person)	First and second surnames (in accordance with document of identity (National Id Document / Passport, …) + " - DNI " + VAT number of public servant
Given name	First name	First name, in accordance with document of identity (National Id Document / Passport, …)
CN, Common Name	First name, surnames and identity (NIF)	First name and two surnames as displayed on identification document (National Id Document/ Passport, …) + " - DNI" + VAT number of the public servant + " (SIG)"
C, Country	Country	C = "ES"
Organization Identifier		Following the technical standard ETSI EN 319 412-1 (VATES + VAT number of the entity)

[7] SerialNumber = e.g.: IDCES-00000000G. 3 characters to indicate the type of document (IDC = national identity document, PAS= passport, etc.) + 2 characters to identify the country (ES) + Identity Number (Printable String)) Size [RFC 5280] 64

Extensions

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