Consorci
Administració Oberta
de Catalunya

Descripció del Perfil de certificats CPIXSA-2 Càrrec opcional

Generalitat de Catalunya

LOCALRET

Control documental

Estat formal	Elaborat per: Chema López		Aprovat per: Francesc Ferrer
Data de creació	08/10/2014		
Control de versions	**Versió:**	2.2	
	Data:	20/01/16	
	Descripció:	Creació del perfil CPIXSA-2 C per a l'EC-SectorPublic	
Nivell accés informació	Pública		
Títol	Descripció del Perfil de certificats CPIXSA-2 Càrrec opcional		
Fitxer	D1112 N-Perfil EC-SectorPublic CPIXSA-2 Càrrec opcional v2r2.doc		
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 2.5 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.		

Índex

1 Descripció del perfil CPIXSA-2 C de l'EC-SectorPublic 4

Descripció del perfil CPIXSA-2 C de l'EC-SectorPublic

Camp	Descripció Contingut	Valor	Obligat
1. X.509 Field			
1.1. Version	v3	2	Sí
1.2. Serial Number	*Integer positiu, establert automàticament per l'EC, que identificarà de manera unívoca el certificat.*		Sí
1.3. Signature Algorithm			Sí
1.3.1. Identifier		1.2.840.113549.1.1.5	Sí
1.3.2. Description		"SHA-1 with RSA Signature"	Sí
1.4. Issuer Distinguished Name	*Establert automàticament per l'EC.*		Sí
1.4.1. Common Name (CN)		"EC-SectorPublic"	Sí
1.4.2. Country (C)		"ES"	Sí
1.4.3. Organization (O)		"CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA"	Sí
1.4.4. Organizational Unit (OU)		"Serveis Públics de Certificació"	Sí
1.5. Validity		Fins a 5 anys	Sí
1.5.1. Not Before	*e.g., "00:00:01 01 September 1999"*		Sí
1.5.2. Not After	*e.g., "23:59:59 31 August 2003"*		Sí
1.6. Subject	*Tots aquests camps es codificaran amb UTF-8*		Sí
1.6.1. Common Name (CN)	*OID: 2.5.4.3*	*"*TCAT P*" + Nom i cognoms del posseïdor de claus* + "|" +	Sí

Camp	Descripció Contingut	Valor	Obligat
		NIF/NIE/Passaport/altre document identificatiu del posseïdor de claus	
1.6.2. Given Name (G)	*OID: 2.5.4.42*	*Nom de pila del posseïdor de claus, conforme al document identificatiu.*	Sí
1.6.3. Surname (SN)	*OID: 2.5.4.4*	*Cognoms del posseïdor de claus, conforme al document identificatiu.*	Sí
1.6.4. Serial Number	*OID: 2.5.4.5*	*A) Número del document identificatiu (NIF/NIE) del posseïdor de claus. O bé:* *B) Número del document nacional d'identitat del país d'origen/Passaport) del posseïdor de claus. O bé:* *C) Número d'altres identificadors, conforme al que estipula la Política general de certificació*[1]	Sí
1.6.5. Country (C)	*OID: 2.5.4.6*	*Codi de 2 lletres del país de l'ens subscriptor.*	Sí

[1] Conforme a la Política general de certificació, apartat "Resolució de conflictes relatius a noms": En **certificats corporatius**, els conflictes de noms dels posseïdors de claus que apareixen identificats amb el seu nom real se solucionen mitjançant la inclusió, en el nom distingit del certificat, de:

- En el cas que l'"Organization" del camp "Subject" (això és, l'ens subscriptor) estigui sotmesa a dret espanyol:
- En el cas de posseïdors de claus nacionals espanyols, el número de DNI del subscriptor.
  V.gr.: (C) = ES; (SN) = #DNI
- En el cas d'estrangers amb algun tipus de vinculació amb Espanya, com ara la residència en territori espanyol, el n número de NIE del subscriptor.
  V.gr.: francés (C) = ES; (SN) = #NIE
  V.gr.: argentino (C) = ES; (SN) = #NIE
- En el cas d'estrangers nacionals d'Estats que són part de l'Acord Schengen i que no disposen de NIE, el número de document nacional d'identitat del país d'origen o de procedència o passaport vigent del subscriptor. També es podrà consignar, abans del número del documento identificador citat, el codi del país del que el subscriptor és nacional, de conformitat amb els paràmetres establerts per la norma ISO 3166 Codes (Countries), separat per un guió.
  V.gr.: italiano (C) = IT; (SN) = #Documento nacional de identitat
  V.gr.: italiano (C) = IT; (SN) = IT-#Documento nacional de identitat
- En el cas d'estrangers nacionals d'Estats que no són part de l'Acord Schengen i que no disposen de NIE, el número de passaport ordinari, diplomàtic, oficial o de servei, del subscriptor vàlidament emès i en vigor. També es podrà consignar, abans del número del document identificador citat, el codi del país del que el subscriptor és nacional, de conformitat amb els paràmetres establerts per la norma ISO 3166 Codes (Countries), separat per un guió.
  V.gr.: chino (C) = CN; (SN) = #Pasaporte
  V.gr.: chino (C) = CN; (SN) = CN-#Pasaporte
- El número de qualsevol altre identificador assignat al posseïdor de claus pel subscriptor.
  V.gr.: un número de col·legiat.
- En cas que l'"Organization" del "Subject" (això és, l'ens subscriptor) no estigui sotmès a dret espanyol, la semàntica del "SerialNumber" dependrà de la normativa aplicable conforme al "countryName" d'aquest ens.

Camp	Descripció Contingut	Valor	Obligat
1.6.6. Organization (O)	*OID: 2.5.4.10*	*Nom legal de l'ens subscriptor*	Sí
1.6.7. Organizational Unit (OU)	*OID: 2.5.4.11*	*Departament/Unitat*	NO
1.6.8. Organizational Unit (OU)	*OID: 2.5.4.11*	"Vegeu https://www.aoc.cat/CATCert/Regulacio"	Sí
1.6.9. Title (T)	*OID: 2.5.4.12*	*Categoria i càrrec del posseïdor de claus*	NO
1.7. Subject Public Key Info			Sí
1.7.1. Min Key Length		2048	Sí
1.7.2. Algorithm ID			Sí
1.7.2.1. Identifier	*OID: 2.5.8.1.1*		Sí
1.7.2.2. Description		X.509 defined RSA encryption algorithm.	Sí
2. X.503v3 Extensions			
2.1. Authority Key Identifier	*OID: 2.5.29.35*		Sí
2.1.1. Key Identifier	*Identificador de la clau pública de l'EC emisora*		
2.2. Subject Key Identifier	*OID: 2.5.29.14*		Sí
2.2.1. Key Identifier	*Identificador de la clau pública del posseïdor de claus*		
2.3. Key Usage	*Aquest camp es marca com **crític***		Sí (i **crític**)
2.3.1. Digital Signature		True ("1")	
2.3.2. Non Repudiation		True ("1")	
2.3.3. Key Encipherment		True ("1")	
2.3.4. Data Encipherment		True ("1")	
2.3.5. Key Agreement		True ("1")	

Camp	Descripció Contingut	Valor	Obligat
2.3.6. Key Certificate Signature		False (“0”)	
2.3.7. CRL Signature		False (“0”)	
2.3.8. Encipher Only		False (“0”)	
2.3.9. Decipher Only		False (“0”)	
2.4. Certificate Policies			Sí
2.4.1. Policy Identifier		1.3.6.1.4.1.15096.1.3.1.86.3	Sí
2.4.2. Policy Qualifier ID			Sí
2.4.2.1. CPS Pointer		https://www.aoc.cat/CATCert/Regulacio	Sí
2.4.2.2. User Notice		"Cert. personal reconegut d’identif., xifratge i sig. avançada per a emp. públic segons la Llei 11/2007, de classe 2 i nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"	Sí
2.5. Subject Alternative Names			Sí
2.5.1. GeneralNames			
2.5.1.1. rfc822Name		*Correu electrònic del posseïdor de claus*	Sí
2.5.1.2. directoryName			
2.5.1.2.1. Atribut privat	*OID: 2.16.724.1.3.5.3.2.1*	“Certificat d’empleat públic, de classe 1, nivell mig.”	Sí
2.5.1.2.2. Atribut privat	*OID: 2.16.724.1.3.5.3.2.2 (Valor idèntic al del camp “Organization” del “Subject”)*	*Nom legal de l’ens subscriptor*	
2.5.1.2.3. Atribut privat	*OID: 2.16.724.1.3.5.3.2.3*	*CIF de l’ens subscriptor*	

Camp	Descripció Contingut	Valor	Obligat
2.5.1.2.4. Atribut privat	*OID: 2.16.724.1.3.5.3.2.4 (Valor idèntic al del camp "serialNumber" del "Subject")*	*Número del document identificatiu (NIF/NIE) del posseïdor de claus*	
2.5.1.2.5. Atribut privat	*OID: 2.16.724.1.3.5.3.2.5*	*Número identificatiu del posseïdor de claus. Es correspon amb el NRP o NIP*	
2.5.1.2.6. Atribut privat	*OID: 2.16.724.1.3.5.3.2.6 (Valor idèntic al del camp "givenName" del "Subject")*	*Nom de pila del posseïdor de claus, conforme al document identificatiu.*	
2.5.1.2.7. Atribut privat	*OID: 2.16.724.1.3.5.3.2.7*	*Primer cognom del posseïdor de claus, conforme al document identificatiu.*	
2.5.1.2.8. Atribut privat	*OID: 2.16.724.1.3.5.3.2.8*	*Segon cognom del posseïdor de claus, conforme al document identificatiu.*	
2.5.1.2.9. Atribut privat	*OID: 2.16.724.1.3.5.3.2.9*	*Correu electrònic del posseïdor de claus*	
2.5.1.2.10. Atribut privat	*OID: 2.16.724.1.3.5.3.2.10*	*Departament/Unitat a la qual està adscrit el posseïdor de claus*	
2.5.1.2.11. Atribut privat	*OID: 2.16.724.1.3.5.3.2.11*	*Categoria i/o càrrec del posseïdor de claus*	
2.6. Extended Key Usage			Sí
2.6.1. emailProtection	*Present*	1.3.6.1.5.5.7.3.4	Sí
2.6.2. TLSWebClientAuth	*Present*	1.3.6.1.5.5.7.3.2	Sí
2.6.3.			
2.7. cRLDistributionPoint			Sí
2.7.1. distributionPoint		http://epscd.catcert.net/crl/ec-sectorpublic.crl	Sí
2.8. Authority Info Access			Sí

Camp	Descripció Contingut	Valor	Obligat
2.8.1. AccessDescription			
2.8.1.1. Access Method	*Id-ad-ocsp*	1.3.6.1.5.5.7.48.1	Sí
2.8.1.2. Access Location		http://ocsp.catcert.cat	Sí
2.9. AccessDescription			
2.9.1.1. Access Method	*id-ad-caIssuers*	1.3.6.1.5.5.7.48.2	Sí
2.9.1.2. Access Location		http://www.catcert.cat/descarrega/ec-sectorpublic.crt	Sí
2.10. QualifiedCertificateStatements			
2.10.1. QcCompliance	*Present*		Sí
2.10.2. QcRetentionPeriod			Sí
2.10.2.1. QcEuRetentionPeriod		15	