Consorci
Administració Oberta
de Catalunya

Descripció del Perfil de certificats CPIXSA-2 IDCat

Generalitat de Catalunya

LOCALRET

Realitzat per: Servei de Certificació Digital - CATCert
Versió: 2.5
Data: 20/01/2016
Arxiu: D1112 N-Perfil CPIXSA-2 IDCat v2r5.doc

Control documental

Estat formal	**Elaborat per:** **Chema López**		**Aprovat per:** **Francesc Ferrer**
Data de creació	23/02/2010		
Control de versions	**Versió:**	2.5	
	Data:	20/01/2016	
	Descripció:	Adaptació del perfil CPIXSA-2 IDCat per a l'EC-Ciutadania	
Nivell accés informació	Pública		
Títol	Descripció del Perfil de certificats CPIXSA-2 IDCat		
Fitxer	D1112 N-Perfil CPIXSA-2 IDCat v2r5.doc		
Control de còpies	Només les còpies disponibles a la web del Consorci AOC 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.		

Index

Descripció del perfil CPIXSA-2 IDCat de l'EC-Ciutadania

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-Ciutadania"	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		4 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*	*Nom i cognoms del posseïdor de claus*	Sí

Camp	Descripció Contingut	Valor	Obligat
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*[1]	Sí
1.6.5. Country (C)	*OID: 2.5.4.6*	*Codi de 2 lletres del país del posseïdor de claus*	Sí
1.6.6. Organizational Unit (OU)	*OID: 2.5.4.11*	"Vegeu https://www.aoc.cat/CATCert/Regulacio"	Sí
1.7. Subject Public Key Info			Sí
1.7.1. Min Key Length		2048	
1.7.2. Algorithm ID			
1.7.2.1. Identifier	*OID: 2.5.8.1.1*		
1.7.2.2. Description		X.509 defined RSA encryption	

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

- En el cas de 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

Camp	Descripció Contingut	Valor	Obligat
		algorithm.	
2. X.503v3 Extensions			Sí
2.1. Authority Key Identifier	*OID: 2.5.29.35*		
2.1.1. Key Identifier	*Identificador de la clau pública de l'EC emisora*		
2.2. Subject Key Identifier	*OID: 2.5.29.14*		
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")	
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		1.3.6.1.4.1.15096.1.3.1.86.1	
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer		https://www.aoc.cat/CATCert/Regulacio	

Camp	Descripció Contingut	Valor	Obligat
2.4.2.2. User Notice		"Certificat personal reconegut d'identificació, xifratge i signatura avançada, de classe 2. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"	
2.5. Subject Alternative Names			
2.5.1. GeneralNames			
2.5.1.1. rfc822Name		*Correu electrònic del posseïdor de claus*	
2.5.1.2. directoryName			
2.5.1.2.1. Common Name (CN)	*OID: 2.5.4.3*	*Nom de pila i cognoms del posseïdor de claus, conforme al document identificatiu.*	
2.5.1.2.2. Serial Number	*OID: 2.5.4.5 (Valor idèntic al del camp "serialNumber" del "Subject")*	*Número del document identificatiu (NIF/NIE/Passaport) del posseïdor de claus*	
2.5.1.2.3. Country (C)	*OID: 2.5.4.6 (Valor idèntic al del camp "Country" del "Subject")*	*Codi de 2 lletres del país del posseïdor de claus*	
2.5.1.2.4. Organization	*OID: 2.5.4.10*	"Consorci Administració Oberta de Catalunya"	
2.5.1.2.5. Organization Unit (OU)	*OID: 2.5.4.11*	"IDCAT"	
2.6. Extended Key Usage			Sí
2.6.1. emailProtection	*Present*	1.3.6.1.5.5.7.3.4	
2.6.2. TLSWebClientAuth	*Present*	1.3.6.1.5.5.7.3.2	
2.7. CRLDistributionPoint			Sí
2.7.1. distributionPoint		http://epscd.catcert.net/crl/ec-ciutadania.crl	
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	
2.8.1.2. Access Location		http://ocsp.catcert.cat	
2.8.2. AccessDescription			
2.8.2.1. Access Method	*id-ad-calssuers*	1.3.6.1.5.5.7.48.2	
2.8.2.2. Access Location		http://www.catcert.cat/descarrega/ec-ciutadania.crt	
2.9. QualifiedCertificateStatements			Sí
2.9.1. QcCompliance	*Present*		
2.9.2. QcRetentionPeriod			
2.9.2.1. QcEuRetentionPeriod		15	