Consorci
Administració Oberta
de Catalunya

Descripció del Perfil de certificats CPPISR-1 Pseudonim Càrrec opcional

Generalitat de Catalunya

LOCALRET

Control documental

Estat formal	Elaborat per: Chema López	Aprovat per: Francesc Ferrer
Data de creació	14/08/2015	
Control de versions	**Versió:**	1.0
	Data:	20/01/16
	Descripció:	Creació del perfil CPPISR-1 Pseudònim Càrrec opcional
Nivell accés informació	Pública	
Títol	D1112 N-Perfil EC-SectorPublic CPPISR-1	
Fitxer	D1112 N-Perfil EC-SectorPublic CPPISR-1 Càrrec opcional v1r0.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.	

Index

Descripció del perfil CPPISR-1 Pseudònim Càrrec Opcional 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.,*		Sí

Camp	Descripció Contingut	Valor	Obligat
	"23:59:59 31 August 2003"		
1.6. Subject	*Tots aquests camps es codificaran amb UTF-8*		Sí
1.6.1. Common Name (CN)	*OID: 2.5.4.3*	*"*CPPISR-1 Pseudònim. Certificat d'empleat públic amb pseudònim*"*	Sí
1.6.2. Pseudonym	*OID: 2.5.4.65*	*Pseudònim del posseïdor de claus*	Sí
1.6.3. Serial Number	*OID: 2.5.4.5*	*Codi identificatiu del posseïdor de claus.*	No
1.6.4. Country (C)	*OID: 2.5.4.6*	*Codi de 2 lletres del país de l'ens subscriptor.*	Sí
1.6.5. Organization (O)	*OID: 2.5.4.10*	*Nom legal de l'ens subscriptor*	Sí
1.6.6. Organizational Unit (OU)	*OID: 2.5.4.11*	*Departament/Unitat*	NO
1.6.7. Organizational Unit (OU)	*OID: 2.5.4.11*	"Vegeu https://www.aoc.cat/CATCert/Regulacio"	Sí
1.6.8. 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

Camp	Descripció Contingut	Valor	Obligat
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”)	Sí
2.3.2. Non Repudiation		True (“1”)	Sí
2.3.3. Key Encipherment		True (“1”)	
2.3.4. Data Encipherment		False (“0”)	
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		1.3.6.1.4.1.15096.1.3.1.81.5.1	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		“Certificat personal reconegut d’identificació i signatura reconeguda amb pseudònim i Càrrec opcional, de classe 1. 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.		*Correu electrònic del posseïdor de claus*	Sí

Camp	Descripció Contingut	Valor	Obligat
rfc822Name			
2.5.1.2. directoryName			
2.5.1.2.1. SerialNumber		*CIF de l'ens subscriptor*	Sí
2.5.1.3. otherName			
2.5.1.3.1. userPrincipalName (UPN)		*Usuari en el domini Windows del posseïdor de claus*	No
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. SmartCardLogon	*Present*		
2.7. cRLDistributionPoint			Sí
2.7.1. distributionPoint		http://epscd.catcert.net/crl/ec-sectorpublic.crl	Sí
2.8. Authority Info Access			Sí
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

Camp	Descripció Contingut	Valor	Obligat
2.10. QualifiedCertificateStatements			
2.10.1. QcCompliance	*Present*		Sí
2.10.2. QcRetentionPeriod			Sí
2.10.2.1. QcEuRetentionPeriod		15	
2.10.3. QcSSCD	*Present*		Sí