



Consorci
Administració Oberta
de Catalunya

Descripció del Perfil de certificats CDA-1 SENM

 Generalitat
de Catalunya

LOCALRET

Control documental

Estat formal	Elaborat per: Chema López	Aprovat per: Francesc Ferrer
Data de creació	23/02/2010	
Control de versions	Versió:	2.6
	Data:	15/04/2015
	Descripció:	Adaptació del perfil CDA-1 SENM per a l'EC-SectorPublic
Nivell accés informació	Pública	
Títol	Descripció del Perfil de certificats CDA-1 SENM	
Fitxer	D1112 N-Perfil EC-SectorPublic CDA-1 SENM v2r6.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 CDA-1 SENM de l'EC-SectorPublic.....	4
---	--	---

Descripció del perfil CDA-1 SENM de l'EC-SectorPublic

Camp	Descripció Contingut	Valor	Obligat
1. X.509 Field			
1.1. Version	v3	2	Sí
1.2. Serial Number	<i>Integer positiu, establert automàticament per l'EC, que identificarà de manera unívoca el certificat.</i>		Sí
1.3. Signature Algorithm			Sí
1.3.1. Identifier		1.2.840.113549.1.1.5	
1.3.2. Description		"SHA-1 with RSA Signature"	
1.4. Issuer Distinguished Name	<i>Establert automàticament per l'EC</i>		Sí
1.4.1. Common Name (CN)		"EC-SectorPublic"	
1.4.2. Country (C)		"ES"	
1.4.3. Organization (O)		"CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA"	
1.4.4. Organizational Unit (OU)		"Serveis Públics de Certificació"	
1.5. Validity		3 anys	Sí
1.5.1. Not Before	<i>e.g., "00:00:01 01 September 1999"</i>		
1.5.2. Not After	<i>e.g., "23:59:59 31 August 2003"</i>		
1.6. Subject	<i>Tots aquests camps es codificaran amb UTF-8</i>		Sí

Camp	Descripció Contingut	Valor	Obligat
1.6.1. Common Name (CN)	OID: 2.5.4.3	Denominació del sistema, aplicació o component d'actuació automatitzada que posseeix el certificat de segell	Sí
1.6.2. GivenName (G)	OID: 2.5.4.42	Nom del responsable	
1.6.3. Surname (SN)	OID: 2.5.4.4	Cognoms del responsable	
1.6.4. Serial Number (SN)	OID: 2.5.4.5	NIF de l'ens subscriptor	Sí
1.6.5. Country (C)	OID: 2.5.4.6	Codi de 2 lletres del país de l'ens subscriptor	Sí
1.6.6. Organization (O)	OID: 2.5.4.10	Nom legal de l'ens subscriptor – Entitat de registre	Sí
1.6.7. Organizational Unit (OU)	OID: 2.5.4.11	Departament/Unitat	
1.6.8. Organizational Unit (OU)	OID: 2.5.4.11	“Certificat de segell electrònic, de classe 1, nivell mig”	Sí
1.6.9. 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 algorithm.	
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		

Camp	Descripció Contingut	Valor	Obligat
2.3. Key Usage	<i>Aquest camp es marca com crític</i>		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		False ("0")	
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		1.3.6.1.4.1.15096.1.3.1.91.1	
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer		https://www.aoc.cat/CATCert/Regulacio	
2.4.2.2. User Notice		"Certificat de segell electrònic amb conformitat amb la llei 11/2007, de classe 1 i nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"	
2.5. Subject Alternative Names			Sí
2.5.1. GeneralNames			
2.5.1.1. rfc822Name		<i>Adreça de correu electrònic per a la formulació de suggeriments i queixes</i>	
2.5.1.2. directoryName			
2.5.1.2.1.	<i>OID: 2.16.724.1.3.5.2.2.</i>	Certificat de segell electrònic, de classe 1, nivell mig	Sí

Camp	Descripció Contingut	Valor	Obligat
Atribut privat	1		
2.5.1.2.2. Atribut privat	OID: 2.16.724.1.3.5.2.2. 2	Nom de l'ens subscriptor, propietari del certificat	Sí
2.5.1.2.3. Atribut privat	OID: 2.16.724.1.3.5.2.2. 3	CIF de l'ens subscriptor.	Sí
2.5.1.2.4. Atribut privat	OID: 2.16.724.1.3.5.2.2. 4	DNI/NIE del responsable del segell	
2.5.1.2.5. Atribut privat	OID: 2.16.724.1.3.5.2.2. 5	Denominació del sistema, aplicació o component d'actuació automatitzada que posseeix el certificat de segell	Sí
2.5.1.2.6. Atribut privat	OID: 2.16.724.1.3.5.2.2. 6	Nom de pila del responsable del certificat	
2.5.1.2.7. Atribut privat	OID: 2.16.724.1.3.5.2.2. 7	Primer cognom del responsable del certificat	
2.5.1.2.8. Atribut privat	OID: 2.16.724.1.3.5.2.2. 8	Segon cognom del responsable del certificat	
2.5.1.2.9. Atribut privat	OID: 2.16.724.1.3.5.2.2. 9	Correu electrònic del responsable del segell	
2.6. Extended Key Usage			Sí
2.6.1. TLSWebClientAuth	Present	1.3.6.1.5.5.7.3.2	
2.6.2. emailProtection	Present	1.3.6.1.5.5.7.3.4	
2.7. cRLDistributionPoint			Sí
2.7.1. distributionPoint		http://epsd.catcert.net/crl/ec-sectorpublic.crl	
2.8. Authority Info Access			Sí
2.8.1. AccessDescription			

Camp	Descripció Contingut	Valor	Obligat
2.8.1.1. Access Method	<i>id-ad-ocsp</i>	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	<i>id-ad-caIssuers</i>	1.3.6.1.5.5.7.48.2	
2.8.2.2. Access Location		http://www.catcert.cat/descarrega/ec-sectorpublic.crt	
2.9. Qualified Certificate Statements			Sí
2.9.1. QcCompliance	<i>Present</i>		
2.9.2. QcRetentionPeriod			
2.9.2.1. QcEuRetentionPeriod		15	