Consorci
Administració Oberta
de Catalunya

Descripció del Perfil de certificats CDS-1 SENM EV (Seu-e Nivell Mig Extended Validation)

Generalitat
de Catalunya

LOCALRET

Control documental

Estat formal	**Elaborat per:** **Servei de Certificació Digital**		**Aprovat per:** **Direcció del Consorci AOC**
Data de creació	23/02/2010		
Control de versions	**Versió:**	2.6	
	Data:	28/10/16	
	Descripció:	Adaptació del perfil CDS-1 SENM EV per a l'EC-SectorPublic	
Nivell accés informació	Pública		
Títol	Adaptació a WebTrust BR i perfils de la *Dirección de Tecnologías de la Información y las Comunicaciones* (DTIC)		
Fitxer	D1112 N-Perfil EC-SectorPublic CDS-1 SENM EV v2r6		
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

Descripció del perfil CDS-1 SENM EV (Seu-e Nivell Mig Extended Validation) 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. <20 octets*		Sí
1.3. Signature Algorithm			Sí
1.3.1. Identifier		1.2.840.113549.1.1.11	
1.3.2. Description	Algorisme de la clau. String UTF8. Size=40	"SHA-256 with RSA Signature"	
1.4. Issuer Distinguished Name	*Establert automàticament per l'EC*		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		2 anys	Sí
1.5.1. Not Before	*e.g., "00:00:01 01 September 2001"*		
1.5.2. Not After	*e.g., "23:59:59 31 August 2003"*		
1.6. Subject	*Tots aquests camps es codificaran amb UTF-8*		Sí

Camp	Descripció Contingut	Valor	Obligat
1.6.1. Common Name (CN)	*OID: 2.5.4.3*	*DNS del servidor (NO adreça IP)*	No
1.6.2. Serial Number	*OID: 2.5.4.5*	*CIF de l'ens subscriptor*	Sí
1.6.3. Country (C)	*OID: 2.5.4.6*	*Codi de 2 lletres del país de l'ens subscriptor*	Sí
1.6.4. Locality (L)	*OID: 2.5.4.7*	*Localitat de l'ens subscriptor*	Sí
1.6.5. Bussiness Category	*OID: 2.5.4.15*	"Government entity"	Sí
1.6.6. Postal Code	*OID:2.5.4.17*	*Codi postal de l'ens subscriptor*	No
1.6.7. State or Province Name	*OID: 2.5.4.8*	*Província de l'ens subscriptor*	Sí
1.6.8. Street Address	*OID: 2.5.4.9*	*Adreça postal de l'ens subscriptor*	No
1.6.9. Organization (O)	*OID: 2.5.4.10*	*Nom legal de l'ens subscriptor, òrgan o entitat administrativa*	Sí
1.6.10. Organizational Unit (OU)	*OID: 2.5.4.11*	*Identificació de la seu-e*	Sí
1.6.11. Organizational Unit (OU)	*OID: 2.5.4.11*	"Certificat de seu electrònica, de classe 1, nivell mig"	Sí
1.6.12. Organizational Unit (OU)	*OID: 2.5.4.11*	"Vegeu https://www.aoc.cat/CATCert/Regulacio"	Sí
1.6.13. Atribut privat	*OID: 1.3.6.1.4.1.311.60.2.1.1*	*Localitat en la que està registrat l'ens subscriptor (si cal)*	Sí
1.6.14. Atribut privat	*OID: 1.3.6.1.4.1.311.60.2.1.2*	*Província en la que està registrat l'ens subscriptor (si cal)*	Sí
1.6.15. Atribut privat	*OID: 1.3.6.1.4.1.311.60.2.1.3*	*País en el que està registrat l'ens subscriptor*	Sí
1.7. Subject Public Key Info			Sí
1.7.1. Min Key Length		2048	
1.7.2. Algorithm ID			

Camp	Descripció Contingut	Valor	Obligat
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*		
2.3. Key Usage	*Aquest camp es marca com **crític***		Sí (i **crític**)
2.3.1. Digital Signature		True ("1")	
2.3.2. Content Commitment		False ("0")	
2.3.3. Non Repudiation		False ("0")	
2.3.4. Key Encipherment		True ("1")	
2.3.5. Data Encipherment		False ("0")	
2.3.6. Key Agreement		True ("0")	
2.3.7. Key Certificate Signature		False ("0")	
2.3.8. CRL Signature		False ("0")	
2.3.9. Encipher Only		False ("0")	
2.3.10. Decipher Only		False ("0")	
2.4. Certificate Policies			Sí
2.4.1. Policy Identifier		1.3.6.1.4.1.15096.1.3.1.51.2	
2.4.2. Policy Qualifier ID			

Camp	Descripció Contingut	Valor	Obligat
2.4.2.1. CPS Pointer		https://www.aoc.cat/CATCert/Regulacio	
2.4.2.2. User Notice		"Certificat de seu electrònica conforme 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. DNS Name	*El contingut d'aquest camp ha de coincidir amb l'especificat al "CommonName" del "Subject", si aquest està present.*	*Nom de Domini DNS de la seu-e.*	Sí
2.5.1.2. DNS Name	*Per a certificats multidomini, aquest camp ha de contenir el nom del Domini DNS alternatiu.*	*Nom de Domini DNS alternatiu de la seu-e.*	No
2.5.1.3. directoryName			
2.5.1.3.1. Atribut privat	*OID: 2.16.724.1.3.5.1.2.1*	"Certificat de seu electrònica, de classe 1, nivell mig".	Sí
2.5.1.3.2. Atribut privat	*OID: 2.16.724.1.3.5.1.2.2*	*Nom de l'ens subscriptor, propietari del certificat*	Sí
2.5.1.3.3. Atribut privat	*OID: 2.16.724.1.3.5.1.2.3*	*CIF de l'ens subscriptor.*	Sí
2.5.1.3.4. Atribut privat	*OID: 2.16.724.1.3.5.1.2.4*	*Breu descripció de la seu-e, indicant el seu nom.*	Sí
2.5.1.3.5. Atribut privat	*OID: 2.16.724.1.3.5.1.2.5 El contingut d'aquest camp ha de coincidir amb l'especificat al "CommonName" del "Subject".*	*Nom de Domini DNS de la seu-e.*	Sí
2.6. Extended Key Usage			Sí

Camp	Descripció Contingut	Valor	Obligat
2.6.1. TLSWebServerAuth	*Autenticació TLS Web server*	1.3.6.1.5.5.7.3.1	
2.7. cRLDistributionPoint			Sí
2.7.1. distributionPoint		http://epscd.catcert.net/crl/ec-sectorpublic.crl	
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	
2.8.1.1.1. 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	
2.8.2.1.1. Access Location		http://www.catcert.cat/descarrega/ec-sectorpublic.crt	