



Consorci
Administració Oberta
de Catalunya

Descripció del Perfil de certificats CDA-1

Control documental

Estat formal	Elaborat per: Chema López	Aprovat per: Francesc Ferrer
Data de creació	23/02/2010	
Control de versions	Versió	2.2
	Data:	20/01/16
	Descripció:	Adaptació del perfil CDA-1 per a l'EC-SectorPublic
Nivell accés informació	Pública	
Títol	Descripció del Perfil de certificats CDA-1	
Fitxer	D1112 N-Perfil EC-SectorPublic CDA-1 v2r2	
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 de l'EC-SectorPublic	4
---	--	---

Descripció del perfil CDA-1 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		4 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</i>		Sí

Camp	Descripció Contingut	Valor	Obligat
	<i>codificaran amb UTF-8</i>		
1.6.1. Common Name (CN)	<i>OID: 2.5.4.3</i>	<i>ID textual de l'aplicació</i>	Sí
1.6.2. Serial Number (SN)	<i>OID: 2.5.4.5</i>	<i>ID numèric del servidor d'aplicació</i>	Sí
1.6.3. Country (C)	<i>OID: 2.5.4.6</i>	<i>Codi de 2 lletres del país de l'ens subscriptor</i>	Sí
1.6.4. Organization (O)	<i>OID: 2.5.4.10</i>	<i>Nom legal de l'ens subscriptor – Entitat de registre</i>	Sí
1.6.5. Organizational Unit (OU)	<i>OID: 2.5.4.11</i>	<i>Departament/Unitat</i>	NO
1.6.6. Organizational Unit (OU)	<i>OID: 2.5.4.11</i>	<i>“Vegeu https://www.aoc.cat/CATCert/Regulacio”</i>	Sí
1.7. Subject Public Key Info			Sí
1.7.1. Min Key Length		2048	
1.7.2. Algorithm ID			
Identifier	<i>OID: 2.5.8.1.1</i>		
Description		X.509 defined RSA encryption algorithm.	
2. X.503v3 Extensions			
2.1. Authority Key Identifier	<i>OID: 2.5.29.35</i>		Sí
2.1.1. Key Identifier	<i>Identificador de la clau pública de l'EC emisora</i>		
2.2. Subject Key Identifier	<i>OID: 2.5.29.14</i>		Sí
2.2.1. Key Identifier	<i>Identificador de la clau pública del posseïdor de claus</i>		
2.3. Key Usage	<i>Aquest camp es marca com crític</i>		Sí (i crític)

Camp	Descripció Contingut	Valor	Obligat
2.3.1. Digital Signature		True ("1")	
2.3.2. NonRepudiation/ Content Commitment		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		1.3.6.1.4.1.15096.1.3.1.91	
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer		https://www.aoc.cat/CATCert/Regulacio	
2.4.2.2. User Notice		"Aquest és un certificat de dispositiu d'aplicació assegurada, de classe 1. 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		Correu electrònic del servei	Sí
2.5.1.2. directoryName			
2.5.1.2.1. SerialNumber	OID: 2.5.4.5	CIF de l'ens subscriptor	Sí

Camp	Descripció Contingut	Valor	Obligat
2.6. Extended Key Usage			Sí
2.6.1. TLSWebClientAuth	<i>Present</i>	1.3.6.1.5.5.7.3.2	
2.6.2. emailProtection	<i>Present</i>	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			
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	
2.9. AccessDescription			
2.9.1.1. Access Method	<i>id-ad-calssuers</i>	1.3.6.1.5.5.7.48.2	
2.9.1.2. Access Location		http://www.catcert.cat/descarrega/ec-sectorpublic.crt	