



Consorci
Administració Oberta
de Catalunya

Descripció del Perfil de certificats CDS-1

 Generalitat
de Catalunya

LOCALRET

Control documental

Estat formal	Elaborat per: Servei de Certificació Digital	Aprovat per: Direcció del Consorci Administració Oberta de Catalunya
Data de creació	23/02/2010	
Control de versions	Versió:	2.4
	Data:	28/10/16
	Descripció:	Adaptació a WebTrust BR i EV
Nivell accés informació	Pública	
Títol	Descripció del Perfil de certificats CDS-1	
Fitxer	D1112 N-Perfil EC-SectorPublic CDS-1 v2r4.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 3.0 Espanya de Creative Commons. Per veure'n una còpia, visiteu https://creativecommons.org/licenses/by-nc-nd/3.0/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 CDS-1 de l'EC-SectorPublic	4
---	--	---

Descripció del perfil CDS-1 de l'EC-SectorPublic

Camp	Descripció Contingut	Valor	Obliga t
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		1.2.840.113549.1.111	
1.3.2. Description		"SHA-256 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		2 anys	Sí
1.5.1. Not Before	<i>e.g., "00:00:01 01 September 2001"</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</i>		Sí

Camp	Descripció Contingut	Valor	Obligat
	UTF-8		
1.6.1. Common Name (CN)	OID: 2.5.4.3	FQDN del servidor	No
1.6.2. Country (C)	OID: 2.5.4.6	Codi de 2 lletres del país de l'ens subscriptor	Sí
1.6.3. State or Province Name	OID: 2.5.4.8	Província de l'ens subscriptor	Sí
1.6.4. Organization (O)	OID: 2.5.4.10	Nom legal de l'ens subscriptor – Entitat de registre	Sí
1.6.5. Organizational Unit (OU)	OID: 2.5.4.11	Departament/Unitat	NO
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			
Identifier	OID: 2.5.8.1.1		
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")	

Camp	Descripció Contingut	Valor	Obligat
2.3.2. Non Repudiation		False ("0")	
2.3.3. Key Encipherment		True ("1")	
2.3.4. Data Encipherment		False ("0")	
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		1.3.6.1.4.1.15096.1.3.1.51	
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 dispositiu servidor segur, de classe 1. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A "	
2.5. Subject Alternative Names			Sí
2.5.1.			
2.5.1.1.			
2.5.1.2. DNS Name	<i>El contingut d'aquest camp ha de coincidir amb l'especificat al "CommonName" del "Subject", si aquest està present.</i>	<i>Nom de Domini DNS de la seu-e.</i>	Sí
2.5.1.3. DNS Name	<i>Per a certificats multidomini, aquest camp ha</i>	<i>Nom de Domini DNS alternatiu de la seu-e.</i>	No

Camp	Descripció Contingut	Valor	Obligat
	<i>de contenir el nom del Domini DNS alternatiu.</i>		
2.5.1.4.			
2.5.1.4.1.			
2.6. Extended Key Usage			Sí
2.6.1. TLSWebServerAuth	<i>Present</i>	1.3.6.1.5.5.7.3.1	
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	
2.8.1.1.1. 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	
2.8.2.1.1. Access Location		http://www.catcert.cat/descarrega/ec-sectorpublic.crt	