

Estructura del certificat CDS-1 d'EC-AL

Control documental

Estat formal	Elaborat per: OFICINA DE POLÍTIQUES	Aprovat per: DIRECCIÓ
Data de creació	23/02/2010	
Control de versions	Data:	23/02/2010
	Descripció:	Creació del document
Nivell accés informació	pública	
Títol	Estructura del certificat CDS-1 d'EC-AL	
Fitxer	D1112 N-Perfil CDS-1 EC-AL.pdf	
Control de còpies	Només les còpies disponibles a la web de CATCert 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

Control documental.....	2
Índex.....	3
1. CDS-1 d'EC-AL.....	4

1. CDS-1 d'EC-AL

Camp	Contingut	Obligat	Crític
1. X.509 Field			
1.1. Version	v3	Sí	
1.2. Serial Number	Establert automàticament per la CA	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 Encryption		
1.4. Issuer Distinguished Name			
1.4.1. Common Name (CN)	EC-AL	Sí	
1.4.2. Country (C)	ES	Sí	
1.4.3. Locality (L)	Passatge de la Concepció 11 08008 Barcelona	Sí	
1.4.4. Organization (O)	Agència Catalana de Certificació (NIF Q-0801176-I)	Sí	
1.4.5. Organizational Unit (OU)	Serveis Públics de Certificació ECV-2	Sí	
1.4.6. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCIC-2 (c)03	Sí	
1.4.7. Organizational Unit (OU)	Administracions Locals de Catalunya	Sí	
1.5. Validity			
1.5.1. Validity Period	4 anys	Sí	
1.6. Subject			
1.6.1. Common Name (CN)	2.5.4.3 Adreça IP o DNS del servidor	Sí	
1.6.2. Country (C)	2.5.4.6 Codi de 2 lletres del país del posseïdor de claus	Sí	
1.6.3. Organization (O)	2.5.4.10 Nom legal del subscriptor - Entitat de Registre	Sí	
1.6.4. Organizational Unit (OU)	2.5.4.11 Departament/Unitat	No	
1.6.5. Organizational Unit (OU)	2.5.4.11 Serveis Públics de Certificació CDS-1	Sí	
1.6.6. Organizational Unit (OU)	2.5.4.11 Vegeu https://www.catcert.cat/verCDS-1 (c)03	Sí	
1.7. Subject Public Key Info			
1.7.1. Min Key Length	1024	Sí	
1.7.2. Algorithm ID		Sí	
1.7.2.1. Identifier	2.5.8.1.1	Sí	
1.7.2.2. Description	X.509 defined RSA encryption algorithm.	Sí	
2. X.509v3 Extensions			
2.1. Authority Key Identifier	2.5.29.35	Sí	
2.2. Subject Key Identifier	2.5.29.14	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	true		
2.3.2. Non Repudiation	false		

Camp	Contingut	Obligat	Crític
2.3.3. Key Encipherment	true		
2.3.4. Data Encipherment	false		
2.3.5. Key Agreement	false		
2.3.6. Key Certificate Signature	false		
2.3.7. CRL Signature	false		
2.3.8. Encipher Only	false		
2.3.9. Decipher Only	false		
2.4. Certificate Policies		Si	
2.4.1. Policy Information			
2.4.1.1. Policy Identifier			
2.4.1.1.1. Identifier	1.3.6.1.4.1.15096.1.3.1.51		
2.4.1.2. Policy Qualifiers			
2.4.1.2.1. CPSuri	https://www.catcert.cat/verCDS-1		
2.4.1.2.2. User Notice	Aquest és un certificat de dispositiu servidor segur de classe 1. Vegeu https://www.catcert.cat/verCDS-1		
2.5. Subject Alternate Name		Si	
2.5.1. General Names			
2.5.1.1. rfc822Name			
2.5.1.1.1. Valor establert	Correu electrònic del webmestre		
2.5.1.2. Directory Name			
2.5.1.2.1. Serial Number	2.5.4.5 NIF del subscriptor		
2.6. ExtendedKeyUsages		Si	
2.6.1. TLSWebServerAuth	Present		
2.7. CRL Distribution Points		Si	
2.7.1. Distribution Point			
2.7.1.1. Distribution Point Name			
2.7.1.1.1. Full Name	http://epsd.catcert.net/crl/ec-al.crl		
2.7.1.1.2. Full Name	http://epsd2.catcert.net/crl/ec-al.crl		
2.8. Authority Information Access		Si	
2.8.1. Access Description			
2.8.1.1. OCSP Access Method			
2.8.1.1.1. Access Location	http://ocsp.catcert.cat		
2.8.2. Access Description			
2.8.2.1. caIssuersAccessMethod			
2.8.2.1.1. Access Location	http://www.catcert.cat/descarrega/al_csrs.crt		
2.9. Netscape Certificate Type		Si	
2.9.1. SSLClient	false		

Camp	Contingut	Obligat	Crític
2.9.2. SSLServer	true		
2.9.3. SMIME	false		
2.9.4. ObjectSigning	false		
2.9.5. Reserved	false		
2.9.6. SSLCA	false		
2.9.7. SMIMECA	false		
2.9.8. ObjectSigningCA	false		