

Estructura del certificat CDS-1 EV d'EC-UR

Control documental

Estat formal	Elaborat per: OFICINA DE POLÍTIQUES	Aprovat per: DIRECCIÓ
Data de creació	07/11/2011	
Control de versions	Data:	07/11/2011
	Descripció:	Adaptació requeriments Microsoft
Nivell accés informació	pública	
Títol	Estructura del certificat CDS-1 EV d'EC-UR	
Fitxer	D1112 N-Perfil CDS-1 EV EC-UR v1r1.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

<i>Control documental</i>	2
<i>Índex</i>	3
1. CDS-1 EV d'EC-UR	4

1. CDS-1 EV d'EC-UR

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-UR	Sí	
1.4.2. Country (C)	ES	Sí	
1.4.3. Locality (L)	Passatge de la Concepcio 11 08008 Barcelona	Sí	
1.4.4. Organization (O)	Agencia Catalana de Certificacio (NIF Q-0801176-I)	Sí	
1.4.5. Organizational Unit (OU)	Serveis Publics de Certificacio 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)	Universitats i Recerca	Sí	
1.5. Validity			
1.5.1. Validity Period	2 anys	Sí	
1.6. Subject			
1.6.1. Common Name (CN)	2.5.4.3 <i>Adreça IP o DNS del servidor</i>	Sí	
1.6.2. Serial Number	2.5.4.5 <i>CIF de l'ens/empresa</i>	Sí	
1.6.3. Country (C)	2.5.4.6 <i>Codi de 2 lletres del país del posseïdor de claus</i>	Sí	
1.6.4. Locality (L)	2.5.4.7 <i>Localitat</i>	Sí	
1.6.5. Business Category	2.5.4.15 <i>Ha de contenir un dels següents strings: a) "V1.0, Clause 5.(b)" quan el titular sigui una organització privada (Private organization). b) "V1.0, Clause 5.(c)" quan el titular sigui un ens públic (Government entity). c) "V1.0, Clause 5.(d)" quan el titular sigui una empresa (Business entity).</i>	Sí	

1.6.6. Postal Code	2.5.4.17 <i>Codi postal</i>	No	
1.6.7. State Or Province Name	2.5.4.8 <i>Província</i>	Sí	
1.6.8. Street Address	2.5.4.9 <i>Adreça postal de l'ens</i>	No	
1.6.9. Organization (O)	2.5.4.10 <i>Nom legal del subscriptor – Entitat de Registre</i>	Sí	
1.6.10. Organizational Unit (OU)	2.5.4.11 <i>Departament/Unitat</i>	No	
1.6.11. Organizational Unit (OU)	2.5.4.11 Serveis Públics de Certificació CDS-1	Sí	
1.6.12. Organizational Unit (OU)	2.5.4.11 Vegeu https://www.catcert.cat/verCDS-1EV(c)03	Sí	
1.6.13. Atribut privat	1.3.6.1.4.1.311.60.2.1.1 <i>Localitat en la que està registrada l'ens/empresa (si cal)</i>	No	
1.6.14. Atribut privat	1.3.6.1.4.1.311.60.2.1.2 <i>Província en la que està registrat l'ens/empresa (si cal)</i>	No	
1.6.15. Atribut privat	1.3.6.1.4.1.311.60.2.1.3 <i>País en el que està registrat l'ens/empresa</i>	Sí	
1.7. Subject Public Key Info			
1.7.1. Min Key Length	2048	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		
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		Sí	
2.4.1. Policy Information			
2.4.1.1. Policy Identifier			
2.4.1.1.1. Identifier	1.3.6.1.4.1.15096.1.3.1.51.4		
2.4.1.2. Policy Qualifiers			
2.4.1.2.1. CPSuri	https://www.catcert.cat/verCDS-1EV		
2.4.1.2.2. User Notice	Aquest és un certificat de dispositiu servidor segur de classe 1 amb Extended Validation. Vegeu https://www.catcert.cat/verCDS-1EV		
2.5. Subject Alternate Name		Sí	
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. DNS Name			
2.5.1.2.1. Valor establert	Nom de Domini DNS de la seu; el contingut d'aquest camp ha de coincidir amb l'especificat al "CommonName" del "Subject"		
2.5.1.3. DNS Name			
2.5.1.3.1. Valor establert	Per a certificats multidomini caldrà que aquest 2n "dnsName" contingui el nom de domini DNS alternatiu		
2.5.1.4. Directory Name			
2.5.1.4.1. Serial Number	2.5.4.5 NIF del subscriptor		
2.6. Issuer Alternative Name		Sí	
2.6.1. General Names			
2.6.1.1.	ec_ur@catcert.net		

rfc822Name			
2.7. ExtendedKeyUsages		Sí	
2.7.1. TLSWebServerAuth	Present		
2.8. CRL Distribution Points		Sí	
2.8.1. Distribution Point			
2.8.1.1. Distribution Point Name			
2.8.1.1.1. Full Name	http://epsdc.catcert.net/crl/ec-ur.crl		
2.9. Authority Information Access		Sí	
2.9.1. Access Description			
2.9.1.1. OCSP Access Method			
2.9.1.1.1. Access Location	http://ocsp.catcert.cat		
2.9.2. Access Description			
2.9.2.1. caIssuersAccessMethod			
2.9.2.1.1. Access Location	http://www.catcert.cat/descarrega/ur_csrs.crt		
2.10. Netscape Certificate Type		Sí	
2.10.1. SSLClient	false		
2.10.2. SSLServer	true		
2.10.3. SMIME	false		
2.10.4. ObjectSigning	false		
2.10.5. Reserved	false		
2.10.6. SSLCA	false		
2.10.7. SMIMECA	false		
2.10.8. ObjectSigningCA	false		