

Estructura del certificat CIO-1 d'EC-ACC

Control documental

Estat formal	Elaborat per: OFICINA DE POLÍTIQUES	Aprovat per: DIRECCIÓ
Data de creació	25/02/2010	
Control de versions	Data:	25/02/2010
	Descripció:	Creació del document
Nivell accés informació	pública	
Títol	Estructura del certificat CIO-1 d'EC-ACC	
Fitxer	D1112 N-Perfil CIO-1 EC-ACC.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. CIO-1 d'EC-ACC.....	4

1. CIO-1 d'EC-ACC

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-ACC	Sí	
1.4.2. Country (C)	ES	Sí	
1.4.3. Organization (O)	Agència Catalana de Certificacio (NIF Q-0801176-I)	Sí	
1.4.4. Organizational Unit (OU)	Serveis Publics de Certificacio	Sí	
1.4.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verarrel (c)03	Sí	
1.4.6. Organizational Unit (OU)	Jerarquia Entitats de Certificacio Catalanes	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 Servei OCSP de EC-ACC	Sí	
1.6.2. Country (C)	2.5.4.6 ES	Sí	
1.6.3. Organization (O)	2.5.4.10 Agència Catalana de Certificacio (NIF Q-0801176-I)	Sí	
1.6.4. Organizational Unit (OU)	2.5.4.11 Serveis Publics de Certificacio CIO-1	Sí	
1.6.5. Organizational Unit (OU)	2.5.4.11 Vegeu https://www.catcert.cat/verCIO-1 (c)05	Sí	
1.6.6. Organizational Unit (OU)	2.5.4.11 Jerarquia Entitats de Certificacio Catalanes	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	true		
2.3.3. Key Encipherment	false		

Camp	Contingut	Obligat	Crític
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	1.3.6.1.4.1.15096.1.3.1.19		
2.4.1.2. Policy Qualifiers			
2.4.1.2.1. CPSuri	https://www.catcert.cat/verCIO-1		
2.4.1.2.2. User Notice	Aquest és un certificat de servei OCSP de classe 1. Vegeu https://www.catcert.cat/verCIO-1		
2.5. Subject Alternate Name		Sí	
2.5.1. General Names			
2.5.1.1. rfc822Name	ocsp_acc@catcert.cat		
2.5.1.2. Directory Name			
2.5.1.2.1. Serial Number	2.5.4.5Q0801176I		
2.6. Issuer Alternative Name		Sí	
2.6.1. General Names			
2.6.1.1. rfc822Name	ec_acc@catcert.net		
2.7. ExtendedKeyUsages		Sí	
2.7.1. OCSP Signing	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://epsd.catcert.net/crl/ec-acc.crl		
2.8.1.1.2. Full Name	http://epsd2.catcert.net/crl/ec-acc.crl		
2.9. Authority Information Access		Sí	
2.9.1. Access Description			
2.9.1.1. caIssuersAccessMethod			
2.9.1.1.1. Access Location	http://www.catcert.cat/descarrega/acc.crt		