Agència Catalana de Certificació

Estructura del certificat CIO

Referència:	ACC-PCIO-001
Versió:	1.1
Data:	14/03/2006

Informació general

Control documental

Projecte:	Agència Catalana de Certificació
Entitat de destinació:	
Títol:	Estructura del certificat CIO
Codi de referència:	D1112 – N. CIO
Versió:	1.1
Data:	14/03/2006
Fitxer:	Estructura certificat CIO v1r1 Final.doc
Eina/es d'edició:	Word 2002
Autor/s:	Alamillo Domingo, Ignacio
Resum:	

Drets d'ús

Estat formal

Preparat per:	Revisat per:	Aprovat per:
Nom: Bonet Andrés, Alba Data: 14/03/2006	Nom: Data:	Nom: Data:

Control de versions

Versió	Data	Autor(s)	Gestió de la Qualitat	Canvis/Comentaris
1.0	11/02/2005	Alamillo	Oliveras	Creació del document
1.1	14/03/2006	Bonet	Ódena	Modificació del camp “Policy Identifier”.

Índex

1. CIO-1 Agència Catalana de Certificació

Camp	Contingut	Obligat	Crític
1. X.509v1 Field			
1.1. Version	v3	Sí	
1.2. Serial Number	Establert automàticament per la CA	Sí	
1.3. Signature Algorithm	SHA-1 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	ES	Sí	
1.4.2. Organization (O)	Agencia Catalana de Certificacio (NIF Q-0801176-I)	Sí	
1.4.3. Organizational Unit (OU)	Serveis Publics de Certificacio	Sí	
1.4.4. Organizational Unit (OU)	Vegeu https://www.catcert.net/verarrel (c)03	Sí	
1.4.5. Organizational Unit (OU)	Jerarquia Entitats de Certificacio Catalanes	Sí	
1.4.6. Common Name (CN)	EC-ACC	Sí	
1.5. Validity	4 anys	Sí	
1.5.1. Not Before	e.g., “00:00:01 01 September 1999”	Sí	
1.5.2. Not After	e.g., “23:59:59 31 August 2003”	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	ES	Sí	
1.6.2. Organization (O)	Agencia Catalana de Certificacio (NIF Q-0801176-I)	Sí	
1.6.3. Organizational Unit (OU)	Serveis Publics de Certificacio CIO-1	Sí	
1.6.4. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCIO-1 (c)05	Sí	
1.6.5. Organizational Unit (OU)	Jerarquia Entitats de Certificacio Catalanes	Sí	
1.6.6. Common Name (CN)	Servei OCSP de l’EC-ACC	Sí	
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. X.509v3 Extensions			
2.1. Authority Key Identifier	Present	Sí	
2.1.1. Key Identifier			

Camp	Contingut	Obligat	Crític
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionat “1”	Sí	
2.3.2. Non Repudiation	No seleccionat “0”		
2.3.3. Key Encipherment	No seleccionat “0”		
2.3.4. Data Encipherment	No seleccionat “0”		
2.3.5. Key Agreement	No seleccionat “0”		
2.3.6. Key Certificate Signature	No seleccionat “0”		
2.3.7. CRL Signature	No seleccionat “0”		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	1.3.6.1.4.1.15096.1.3.1.19	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://www.catcert.net/verCIO-1	Sí	
2.4.2.2. User Notice	Aquest és un certificat de servei OCSP de classe 1. Vegeu https://www.catcert.net/verCIO-1	Sí	
2.5. Subject Alternate Names		Sí	
2.5.1. rfc822Name	ocsp_acc@catcert.net	Sí	
2.5.2. Serial Number	Q-0801176-I	Sí	
2.6. Issuer Alternative Name		Sí	
2.6.1. rfc822Name	ec_acc@catcert.net	Sí	
2.7. Extended Key Usage		Sí	
2.7.1. OCSPSigning	Present	Sí	
2.8. cRLDistributionPoint		Sí	
2.8.1. distributionPoint	http://epscd.catcert.net/crl/ec-acc.crl	Sí	
2.8.2. distributionPoint	http://epscd2.catcert.net/crl/ec-acc.crl	Sí	

2. CIO-1 Secretaria Administració i Funció Pública

Camp	Contingut	Obligat	Crític
1. X.509v1 Field			
1.1. Version	v3	Sí	
1.2. Serial Number	Establert automàticament per la CA	Sí	
1.3. Signature Algorithm	SHA-1 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	ES	Sí	
1.4.2. Organization (O)	Agencia Catalana de Certificacio (NIF Q-0801176-I)	Sí	
1.4.3. Organizational Unit (OU)	Pasatge de la Concepcio 11 08008 Barcelona	Sí	
1.4.4. Organizational Unit (OU)	Serveis Publics de Certificacio ECV-2	Sí	
1.4.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCIC-2 (c)03	Sí	
1.4.6. Organizational Unit (OU)	Secretaria Administracio i Funcio Publica	Sí	
1.4.7. Common Name (CN)	EC-SAFP	Sí	
1.5. Validity	4 anys	Sí	
1.5.1. Not Before	e.g., “00:00:01 01 September 1999”	Sí	
1.5.2. Not After	e.g., “23:59:59 31 August 2003”	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	ES	Sí	
1.6.2. Organization (O)	Agencia Catalana de Certificacio (NIF Q-0801176-I)	Sí	
1.6.3. Organizational Unit (OU)	Serveis Publics de Certificacio CIO-1	Sí	
1.6.4. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCIO-1 (c)05	Sí	
1.6.5. Organizational Unit (OU)	Secretaria Administracio i Funcio Publica	Sí	
1.6.6. Common Name (CN)	Servei OCSP de l’EC-SAFP	Sí	
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. X.509v3 Extensions			
2.1. Authority Key Identifier	Present	Sí	

Camp	Contingut	Obligat	Crític
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionat “1”	Sí	
2.3.2. Non Repudiation	No seleccionat “0”		
2.3.3. Key Encipherment	No seleccionat “0”		
2.3.4. Data Encipherment	No seleccionat “0”		
2.3.5. Key Agreement	No seleccionat “0”		
2.3.6. Key Certificate Signature	No seleccionat “0”		
2.3.7. CRL Signature	No seleccionat “0”		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	1.3.6.1.4.1.15096.1.3.1.19	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://www.catcert.net/verCIO-1	Sí	
2.4.2.2. User Notice	Aquest és un certificat de servei OCSP de classe 1. Vegeu https://www.catcert.net/verCIO-1	Sí	
2.5. Subject Alternate Names		Sí	
2.5.1. rfc822Name	ocsp_safp@catcert.net	Sí	
2.5.2. Serial Number	Q-0801176-I	Sí	
2.6. Issuer Alternative Name		Sí	
2.6.1. rfc822Name	ec_safp@catcert.net	Sí	
2.7. Extended Key Usage		Sí	
2.7.1. OCSPSigning	Present	Sí	
2.8. cRLDistributionPoint		Sí	
2.8.1. distributionPoint	http://epscd.catcert.net/crl/ec-safp.crl	Sí	
2.8.2. distributionPoint	http://epscd2.catcert.net/crl/ec-safp.crl	Sí	

3. CIO-1 Administracions Locals de Catalunya

Camp	Contingut	Obligat	Crític
1. X.509v1 Field			
1.1. Version	v3	Sí	
1.2. Serial Number	Establert automàticament per la CA	Sí	
1.3. Signature Algorithm	SHA-1 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	ES	Sí	
1.4.2. Organization (O)	Agencia Catalana de Certificacio (NIF Q-0801176-I)	Sí	
1.4.3. Organizational Unit (OU)	Pasatge de la Concepcio 11 08008 Barcelona	Sí	
1.4.4. Organizational Unit (OU)	Serveis Publics de Certificacio ECV-2	Sí	
1.4.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCIC-2 (c)03	Sí	
1.4.6. Organizational Unit (OU)	Administracions Locals de Catalunya	Sí	
1.4.7. Common Name (CN)	EC-AL	Sí	
1.5. Validity	4 anys	Sí	
1.5.1. Not Before	e.g., “00:00:01 01 September 1999”	Sí	
1.5.2. Not After	e.g., “23:59:59 31 August 2003”	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	ES	Sí	
1.6.2. Organization (O)	Agencia Catalana de Certificacio (NIF Q-0801176-I)	Sí	
1.6.3. Organizational Unit (OU)	Serveis Publics de Certificacio CIO-1	Sí	
1.6.4. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCIO-1 (c)05	Sí	
1.6.5. Organizational Unit (OU)	Administracions Locals de Catalunya	Sí	
1.6.6. Common Name (CN)	Servei OCSP de l’EC-AL	Sí	
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. X.509v3 Extensions			
2.1. Authority Key Identifier	Present	Sí	

Camp	Contingut	Obligat	Crític
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionat “1”	Sí	
2.3.2. Non Repudiation	No seleccionat “0”		
2.3.3. Key Encipherment	No seleccionat “0”		
2.3.4. Data Encipherment	No seleccionat “0”		
2.3.5. Key Agreement	No seleccionat “0”		
2.3.6. Key Certificate Signature	No seleccionat “0”		
2.3.7. CRL Signature	No seleccionat “0”		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	1.3.6.1.4.1.15096.1.3.1.19	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://www.catcert.net/verCIO-1	Sí	
2.4.2.2. User Notice	Aquest és un certificat de servei OCSP de classe 1. Vegeu https://www.catcert.net/verCIO-1	Sí	
2.5. Subject Alternate Names		Sí	
2.5.1. rfc822Name	ocsp_al@catcert.net	Sí	
2.5.2. Serial Number	Q-0801176-I	Sí	
2.6. Issuer Alternative Name		Sí	
2.6.1. rfc822Name	ec_al@catcert.net	Sí	
2.7. Extended Key Usage		Sí	
2.7.1. OCSPSigning	Present	Sí	
2.8. cRLDistributionPoint		Sí	
2.8.1. distributionPoint	http://epscd.catcert.net/crl/ec-al.crl	Sí	
2.8.2. distributionPoint	http://epscd2.catcert.net/crl/ec-al.crl	Sí	

4. CIO-1 Entitat pública de certificació de ciutadans

Camp	Contingut	Obligat	Crític
1. X.509v1 Field			
1.1. Version	v3	Sí	
1.2. Serial Number	Establert automàticament per la CA	Sí	
1.3. Signature Algorithm	SHA-1 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	ES	Sí	
1.4.2. Organization (O)	Agencia Catalana de Certificacio (NIF Q-0801176-I)	Sí	
1.4.3. Organizational Unit (OU)	Pasatge de la Concepcio 11 08008 Barcelona	Sí	
1.4.4. Organizational Unit (OU)	Serveis Publics de Certificacio ECV-2	Sí	
1.4.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCIC-2 (c)03	Sí	
1.4.6. Organizational Unit (OU)	Entitat pública de certificació de ciutadans	Sí	
1.4.7. Common Name (CN)	EC-IDCat	Sí	
1.5. Validity	4 anys	Sí	
1.5.1. Not Before	e.g., “00:00:01 01 September 1999”	Sí	
1.5.2. Not After	e.g., “23:59:59 31 August 2003”	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	ES	Sí	
1.6.2. Organization (O)	Agencia Catalana de Certificacio (NIF Q-0801176-I)	Sí	
1.6.3. Organizational Unit (OU)	Serveis Publics de Certificacio CIO-1	Sí	
1.6.4. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCIO-1 (c)05	Sí	
1.6.5. Organizational Unit (OU)	Entitat pública de certificació de ciutadans	Sí	
1.6.6. Common Name (CN)	Servei OCSP de l’EC-IDCat	Sí	
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. X.509v3 Extensions			
2.1. Authority Key Identifier	Present	Sí	

Camp	Contingut	Obligat	Crític
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionat “1”	Sí	
2.3.2. Non Repudiation	No seleccionat “0”		
2.3.3. Key Encipherment	No seleccionat “0”		
2.3.4. Data Encipherment	No seleccionat “0”		
2.3.5. Key Agreement	No seleccionat “0”		
2.3.6. Key Certificate Signature	No seleccionat “0”		
2.3.7. CRL Signature	No seleccionat “0”		
2.4. Certificate Policies		Sí	
2.4.1. Policy Identifier	1.3.6.1.4.1.15096.1.3.1.19	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://www.catcert.net/verCIO-1	Sí	
2.4.2.2. User Notice	Aquest és un certificat de servei OCSP de classe 1. Vegeu https://www.catcert.net/verCIO-1	Sí	
2.5. Subject Alternate Names		Sí	
2.5.1. rfc822Name	ocsp_idcat@catcert.net	Sí	
2.5.2. Serial Number	Q-0801176-I	Sí	
2.6. Issuer Alternative Name		Sí	
2.6.1. rfc822Name	ec_idcat@catcert.net	Sí	
2.7. Extended Key Usage		Sí	
2.7.1. OCSPSigning	Present	Sí	
2.8. cRLDistributionPoint		Sí	
2.8.1. distributionPoint	http://epscd.catcert.net/crl/ec-idcat.crl	Sí	
2.8.2. distributionPoint	http://epscd2.catcert.net/crl/ec-idcat.crl	Sí	