Agència Catalana
de Certificació

Estructura del certificat CDA

Referència: D1112 N-Perfil CDA
Versió: 2.8
Data: 15/10/2007

Informació general

Control documental

Projecte:	Agència Catalana de Certificació
Entitat de destinació:	
Títol:	Estructura del certificat CDA
Codi de referència:	
Versió:	2.8
Data:	15/10/2007
Fitxer:	D1112 N-Perfil CDA v2r8 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: Chema López Data: 15/10/2007	Nom: Chema López Data: 15/10/2007	Nom: Data:

Control de versions

Versió	Data	Autor(s)	Gestió de la Qualitat	Canvis/Comentaris
1.0	10/07/2003	Alamillo	Oliveras	Creació del document
2.0	22/07/2003	Alamillo	Oliveras	Canvi en termini de validesa
2.1	13/01/2004	Alamillo	Oliveras	Afegir EC-UR
2.2	03/12/2004	Alamillo	Oliveras	Canvi en durada de certificats i afegir OCSP
2.3	26/04/2005	Alamillo	Oliveras	Afegir EC-URV. Eliminar algorisme MD5 de tots els perfils.
2.4	13/03/2006	Bonet	Odena	Correcció del “rfc822Name”
2.5	28/12/2006	Bonet	Odena	Afegir EC-Parlament.
2.6	26/07/2007	AIR		Modificació camp "2.3.4. Data Encipherment"
2.7	17/09/2007	AIR		Camp OU com opcional
2.8	15/10/2007	López		Correció d’enllaços

Índex

Estructura del certificat CDA *1*
Informació general *2*
Control documental 2
Drets d'ús 2
Estat formal 2
Control de versions 3
Índex *4*
1. CDA-1 D'EC-SAFP *5*
2. CDA-1 d'EC-AL *8*
3. CDA-1 d'EC-UR *11*
4. CDA-1 d'EC-URV *14*
5. CDA-1 d'EC-Parlament *17*

1. CDA-1 D'EC-SAFP

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	SHA-1 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	ES	Sí	
1.4.2. Organization (O)	Agència Catalana de Certificació (NIF Q-0801176-I)	Sí	
1.4.3. Locality (L)	Passatge de la Concepció 11 08008 Barcelona	Sí	
1.4.4. Organizational Unit (OU)	Serveis Públics de Certificació 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 Administració i Funció Pública	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)	Nom legal del subscriptor – Entitat de Registre	Sí	
1.6.3. Organizational Unit (OU)	Departament/Unitat	NO	
1.6.4. Organizational Unit (OU)	Serveis Públics de Certificació CDA-1	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCDA-1 (c)03	Sí	
1.6.6. Serial Number	ID numèric del servidor d'aplicació		
1.6.7. Common Name (CN)	ID textual del servidor d'aplicació	Sí	
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	

Camp	Contingut	Obligat	Crític
2. X.509v3 Extensions			
2.1. Authority Key Identifier	Present	Sí	
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	Seleccionat “1”	Sí	
2.3.4. Data Encipherment	Seleccionat “1”	SÍ	
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	1.3.6.1.4.1.15096.1.3.1.91	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://www.catcert.net/verCDA-1	Sí	
2.4.2.2. User Notice	Aquest és un certificat de dispositiu d’aplicació assegurada de classe 1. Vegeu https://www.catcert.net/verCDA-1	Sí	
2.5. Subject Alternate Names		Sí	
2.5.1. rfc822Name	Correu electrònic del servei	Sí	
2.5.2. Serial Number	NIF del subscriptor	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. emailProtection	Present	Sí	
2.7.2. clientAuth	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	
2.9. NetscapeCertType	SSL client S/MIME	Sí	

Camp	Contingut	Obligat	Crític
2.10. Authority Info Access		Sí	
2.10.1. Access Method	id-ad-ocsp	Sí	
2.10.2. Access Location	http://ocsp.catcert.net	Sí	

2. CDA-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	SHA-1 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	ES	Sí	
1.4.2. Organization (O)	Agència Catalana de Certificació (NIF Q-0801176-I)	Sí	
1.4.3. Locality (L)	Passatge de la Concepció 11 08008 Barcelona	Sí	
1.4.4. Organizational Unit (OU)	Serveis Públics de Certificació 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)	Nom legal del subscriptor – Entitat de Registre	Sí	
1.6.3. Organizational Unit (OU)	Departament/Unitat	NO	
1.6.4. Organizational Unit (OU)	Serveis Públics de Certificació CDA-1	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCDA-1 (c)03	Sí	
1.6.6. Serial Number	ID numèric del servidor d'aplicació		
1.6.7. Common Name (CN)	ID textual del servidor d'aplicació	Sí	
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	

Camp	Contingut	Obligat	Crític
2. X.509v3 Extensions			
2.1. Authority Key Identifier	Present	Sí	
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	Seleccionat “1”	Sí	
2.3.4. Data Encipherment	Seleccionat “1”	Sí	
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	1.3.6.1.4.1.15096.1.3.1.91	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://www.catcert.net/verCDA-1	Sí	
2.4.2.2. User Notice	Aquest és un certificat de dispositiu d’aplicació assegurada de classe 1. Vegeu https://www.catcert.net/verCDA-1	Sí	
2.5. Subject Alternate Names		Sí	
2.5.1. rfc822Name	Correu electrònic del servei	Sí	
2.5.2. Serial Number	NIF del subscriptor	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. emailProtection	Present	Sí	
2.7.2. clientAuth	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	
2.9. NetscapeCertType	SSL client S/MIME	Sí	

Camp	Contingut	Obligat	Crític
2.10. Authority Info Access		Sí	
2.10.1. Access Method	id-ad-ocsp	Sí	
2.10.2. Access Location	http://ocsp.catcert.net	Sí	

3. CDA-1 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	SHA-1 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	ES	Sí	
1.4.2. Organization (O)	Agència Catalana de Certificació (NIF Q-0801176-I)	Sí	
1.4.3. Locality (L)	Passatge de la Concepció 11 08008 Barcelona	Sí	
1.4.4. Organizational Unit (OU)	Serveis Públics de Certificació 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)	Universitats i Recerca	Sí	
1.4.7. Common Name (CN)	EC-UR	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)	Nom legal del subscriptor – Entitat de Registre	Sí	
1.6.3. Organizational Unit (OU)	Departament/Unitat	NO	
1.6.4. Organizational Unit (OU)	Serveis Públics de Certificació CDA-1	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCDA-1 (c)03	Sí	
1.6.6. Serial Number	ID numèric del servidor d'aplicació		
1.6.7. Common Name (CN)	ID textual del servidor d'aplicació	Sí	
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	

Camp	Contingut	Obligat	Crític
2. X.509v3 Extensions			
2.1. Authority Key Identifier	Present	Sí	
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	Seleccionat “1”	Sí	
2.3.4. Data Encipherment	Seleccionat “1”	Sí	
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	1.3.6.1.4.1.15096.1.3.1.91	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://www.catcert.net/verCDA-1	Sí	
2.4.2.2. User Notice	Aquest és un certificat de dispositiu d’aplicació assegurada de classe 1. Vegeu https://www.catcert.net/verCDA-1	Sí	
2.5. Subject Alternate Names		Sí	
2.5.1. rfc822Name	Correu electrònic del servei	Sí	
2.5.2. Serial Number	NIF del subscriptor	Sí	
2.6. Issuer Alternative Name		Sí	
2.6.1. rfc822Name	ec_ur@catcert.net	Sí	
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Present	Sí	
2.7.2. clientAuth	Present	Sí	
2.8. cRLDistributionPoint		Sí	
2.8.1. distributionPoint	http://epscd.catcert.net/crl/ec-ur.crl	Sí	
2.8.2. distributionPoint	http://epscd2.catcert.net/crl/ec-ur.crl	Sí	
2.9. NetscapeCertType	SSL client S/MIME	Sí	

Camp	Contingut	Obligat	Crític
2.10. Authority Info Access		Sí	
2.10.1. Access Method	id-ad-ocsp	Sí	
2.10.2. Access Location	http://ocsp.catcert.net	Sí	

4. CDA-1 d'EC-URV

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	SHA-1 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	ES	Sí	
1.4.2. Organization (O)	Agència Catalana de Certificació (NIF Q-0801176-I)	Sí	
1.4.3. Locality (L)	Passatge de la Concepció 11 08008 Barcelona	Sí	
1.4.4. Organizational Unit (OU)	Serveis Públics de Certificació ECV-3	Sí	
1.4.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCIC-3 (c)05	Sí	
1.4.6. Organizational Unit (OU)	Universitat Rovira i Virgili	Sí	
1.4.7. Common Name (CN)	EC-URV	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)	Nom legal del subscriptor – Entitat de Registre	Sí	
1.6.3. Organizational Unit (OU)	Departament/Unitat	NO	
1.6.4. Organizational Unit (OU)	Serveis Públics de Certificació CDA-1	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCDA-1 (c)03	Sí	
1.6.6. Serial Number	ID numèric del servidor d'aplicació		
1.6.7. Common Name (CN)	ID textual del servidor d'aplicació	Sí	
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	

Camp	Contingut	Obligat	Crític
2. X.509v3 Extensions			
2.1. Authority Key Identifier	Present	Sí	
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	Seleccionat “1”	Sí	
2.3.4. Data Encipherment	Seleccionat “1”	Sí	
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	1.3.6.1.4.1.15096.1.3.1.91	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://www.catcert.net/verCDA-1	Sí	
2.4.2.2. User Notice	Aquest és un certificat de dispositiu d’aplicació assegurada de classe 1. Vegeu https://www.catcert.net/verCDA-1	Sí	
2.5. Subject Alternate Names		Sí	
2.5.1. rfc822Name	Correu electrònic del servei	Sí	
2.5.2. Serial Number	NIF del subscriptor	Sí	
2.6. Issuer Alternative Name		Sí	
2.6.1. rfc822Name	ec_urv@catcert.net	Sí	
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Present	Sí	
2.7.2. clientAuth	Present	Sí	
2.8. cRLDistributionPoint		Sí	
2.8.1. distributionPoint	http://epscd.catcert.net/crl/ec-urv.crl	Sí	
2.8.2. distributionPoint	http://epscd2.catcert.net/crl/ec-urv.crl	Sí	
2.9. NetscapeCertType	SSL client S/MIME	Sí	

Camp	Contingut	Obligat	Crític
2.10. Authority Info Access		Sí	
2.10.1. Access Method	id-ad-ocsp	Sí	
2.10.2. Access Location	http://ocsp.catcert.net	Sí	

5. CDA-1 d'EC-Parlament

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	SHA-1 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	ES	Sí	
1.4.2. Organization (O)	Agència Catalana de Certificació (NIF Q-0801176-I)	Sí	
1.4.3. Locality (L)	Passatge de la Concepció 11 08008 Barcelona	Sí	
1.4.4. Organizational Unit (OU)	Serveis Públics de Certificació 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)	Parlament de Catalunya	Sí	
1.4.7. Common Name (CN)	EC-Parlament	Sí	
1.5. Validity	4 anys	Sí	
1.5.1. Not Before	e.g., "00:00:01 01 September 2006"	Sí	
1.5.2. Not After	e.g., "23:59:59 31 August 2010"	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	ES	Sí	
1.6.2. Organization (O)	Nom legal del subscriptor – Entitat de Registre	Sí	
1.6.3. Organizational Unit (OU)	Departament/Unitat	NO	
1.6.4. Organizational Unit (OU)	Serveis Públics de Certificació CDA-1	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCDA-1 (c)03	Sí	
1.6.6. Serial Number	ID numèric del servidor d'aplicació		
1.6.7. Common Name (CN)	ID textual del servidor d'aplicació	Sí	
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	

Camp	Contingut	Obligat	Crític
2. X.509v3 Extensions			
2.1. Authority Key Identifier	Present	Sí	
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	Seleccionat “1”	Sí	
2.3.4. Data Encipherment	Seleccionat “1”	Sí	
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	1.3.6.1.4.1.15096.1.3.1.91	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://www.catcert.net/verCDA-1	Sí	
2.4.2.2. User Notice	Aquest és un certificat de dispositiu d’aplicació assegurada de classe 1. Vegeu https://www.catcert.net/verCDA-1	Sí	
2.5. Subject Alternate Names		Sí	
2.5.1. rfc822Name	Correu electrònic del servei	Sí	
2.5.2. Serial Number	NIF del subscriptor	Sí	
2.6. Issuer Alternative Name		Sí	
2.6.1. rfc822Name	ec_parlament@catcert.net	Sí	
2.7. Extended Key Usage		Sí	
2.7.1. emailProtection	Present	Sí	
2.7.2. clientAuth	Present	Sí	
2.8. cRLDistributionPoint		Sí	
2.8.1. distributionPoint	http://epscd.catcert.net/crl/ec-parlament.crl	Sí	
2.8.2. distributionPoint	http://epscd2.catcert.net/crl/ec-parlament.crl	Sí	
2.9. NetscapeCertType	SSL client S/MIME	Sí	

Camp	Contingut	Obligat	Crític
2.10. Authority Info Access		Sí	
2.10.1. Access Method	id-ad-ocsp	Sí	
2.10.2. Access Location	http://ocsp.catcert.net	Sí	