Agència Catalana
de Certificació

Estructura del certificat CPX

Referència: D1112 N-Perfil CPX
Versió: 2.5
Data: 15/10/2007

Informació general

Control documental

Projecte:	Agència Catalana de Certificació
Entitat de destinació:	
Títol:	Estructura del certificat CPX
Codi de referència:	
Versió:	2.5
Data:	15/10/2007
Fitxer:	D1112 N-Perfil CPX v2r5 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: ISIGMA Data: 15/10/2007	Nom: Data:	Nom: Data:

Control de versions

Versió	Data	Autor(s)	Gestió de la Qualitat	Canvis/Comentaris
1.0	07/03/2003	Alamillo	Oliveras	Creació del document
2.0	08/10/2003	Alamillo	Oliveras	Adaptació a format AEAT alternativa 2, i addició d'adreça OCSP
2.1	03/12/2004	Alamillo	Oliveras	Canvi en la durada dels certificats
2.2	07/09/3005	Alamillo	Odena	Canvi en policy text dels certificats. Eliminació de MD5
2.3	16/03/2006	Bonet	Odena	Modificació dels camps "rfc822Name" i "Serial Number" del Subject.
2.4	17/09/2007	AIR		Camp OU com opcional
2.5	15/10/2007	ISIGMA		Correcció d'enllaços

Índex

Estructura del certificat CPX *1*
Informació general *2*
Control documental 2
Drets d'ús 2
Estat formal 2
Control de versions 3
Índex *4*
1. CPX-1 d'EC-SAFP *5*
2. CPX-1 d'EC-AL *8*
3. CPX-2 Individual d'EC-SAFP *11*
4. CPX-2 Individual d'EC-AL *14*
5. CPX-2 Col·lectiu d'EC-SAFP *17*
6. CPX-2 Col·lectiu d'EC-AL *20*

1. CPX-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)	De conformitat amb la Política General de Certificació	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 CPX-1	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCPX-1 (c)03	Sí	
1.6.6. Surname	Cognoms del posseïdor de claus	Sí	
1.6.7. Given Name	Nom del posseïdor de claus		
1.6.8. Serial Number	Segons Política General de Certificació	Sí	
1.6.9. Common Name (CN)	"CPX-1 " + nom del posseïdor de claus en text lliure	Sí	

Camp	Contingut	Obligat	Crític
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			
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	No seleccionat “0”		
2.3.2. Non Repudiation	No seleccionat “0”		
2.3.3. Key Encipherment	Seleccionat “1”	Sí	
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. Qualified Certificate Statements		Sí	
2.4.1. qCStatement OID	0.4.0.1862.1.1	Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.15096.1.3.1.41	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCPX-1	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal de xifrat de classe 1. Vegeu https://www.catcert.net/verCPX-1	Sí	
2.6. Subject Alternate Names		Sí	
2.6.1. rfc822Name	Correu electrònic del posseïdor de claus	Sí	
2.6.2. Serial Number	NIF del subscriptor	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	ec_safp@catcert.net	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Present	Sí	
2.8.2. clientAuth	Present	Sí	

Camp	Contingut	Obligat	Crític
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	http://epscd.catcert.net/crl/ec-safp.crl	Sí	
2.9.2. distributionPoint	http://epscd2.catcert.net/crl/ec-safp.crl	Sí	
2.10. NetscapeCertType	SSL client S/MIME	Sí	
2.11. Authority Info Access		Sí	
2.11.1. Access Method	id-ad-ocsp	Sí	
2.11.2. Access Location	http://ocsp.catcert.net	Sí	

2. CPX-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)	De conformitat amb la Política General de Certificació	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 CPX-1	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCPX-1 (c)03	Sí	
1.6.6. Surname	Cognoms del posseïdor de claus	Sí	
1.6.7. Given Name	Nom del posseïdor de claus	Sí	
1.6.8. Serial Number	Segons Política General de Certificació	Sí	
1.6.9. Common Name (CN)	"CPX-1 " + Nom del posseïdor de claus en text lliure	Sí	

Camp	Contingut	Obligat	Crític
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			
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	No seleccionat “0”		
2.3.2. Non Repudiation	No seleccionat “0”		
2.3.3. Key Encipherment	Seleccionat “1”	Sí	
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. Qualified Certificate Statements		Sí	
2.4.1. qCStatement OID	0.4.0.1862.1.1	Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.15096.1.3.1.41	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCPX-1	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal de xifrat de classe 1. Vegeu https://www.catcert.net/verCPX-1	Sí	
2.6. Subject Alternate Names		Sí	
2.6.1. rfc822Name	Correu electrònic del posseïdor de claus	Sí	
2.6.2. Serial Number	NIF del subscriptor	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	ec_al@catcert.net	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Present	Sí	
2.8.2. clientAuth	Present	Sí	

Camp	Contingut	Obligat	Crític
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	http://epscd.catcert.net/crl/ec-al.crl	Sí	
2.9.2. distributionPoint	http://epscd2.catcert.net/crl/ec-al.crl	Sí	
2.10. NetscapeCertType	SSL client S/MIME	Sí	
2.11. Authority Info Access		Sí	
2.11.1. Access Method	id-ad-ocsp	Sí	
2.11.2. Access Location	http://ocsp.catcert.net	Sí	

3. CPX-2 Individual 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)	De conformitat amb la Política General de Certificació	Sí	
1.6.2. Organizational Unit (OU)	Serveis Públics de Certificació CPX-2	Sí	
1.6.3. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCPX-2 (c)03	NO	
1.6.4. Surname	Cognoms del subscriptor	Sí	
1.6.5. Given Name	Nom del subscriptor	Sí	
1.6.6. Serial Number	Segons Política General de Certificació	Sí	
1.6.7. Common Name (CN)	"CPX-2 Ind " + Nom del subscriptor en text lliure	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	No seleccionat “0”		
2.3.2. Non Repudiation	No seleccionat “0”		
2.3.3. Key Encipherment	Seleccionat “1”	Sí	
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. Qualified Certificate Statements		Sí	
2.4.1. qCStatement OID	0.4.0.1862.1.1	Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.15096.1.3.1.42	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCPX-2	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal de xifrat de classe 2. Vegeu https://www.catcert.net/verCPX-2	Sí	
2.6. Subject Alternate Names		Sí	
2.6.1. rfc822Name	Correu electrònic del subscriptor del certificat	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	ec_safp@catcert.net	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Present	Sí	
2.8.2. clientAuth	Present	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	http://epscd.catcert.net/crl/ec-safp.crl	Sí	
2.9.2. distributionPoint	http://epscd2.catcert.net/crl/ec-safp.crl	Sí	

Camp	Contingut	Obligat	Crític
2.10. NetscapeCertType	SSL client S/MIME	Sí	
2.11. Authority Info Access		Sí	
2.11.1. Access Method	id-ad-ocsp	Sí	
2.11.2. Access Location	http://ocsp.catcert.net	Sí	

4. CPX-2 Individual 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)	De conformitat amb la Política General de Certificació	Sí	
1.6.2. Organizational Unit (OU)	Serveis Públics de Certificació CPX-2	Sí	
1.6.3. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCPX-2 (c)03	NO	
1.6.4. Surname	Cognoms del subscriptor	Si	
1.6.5. Given Name	Nom del subscriptor	Sí	
1.6.6. Serial Number	Segons Política General de Certificació	Sí	
1.6.7. Common Name (CN)	"CPX-2 Ind " + Nom del subscriptor en text lliure	Sí	
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. X.509v3 Extensions			

Camp	Contingut	Obligat	Crític
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	No seleccionat “0”		
2.3.2. Non Repudiation	No seleccionat “0”		
2.3.3. Key Encipherment	Seleccionat “1”	Sí	
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. Qualified Certificate Statements		Sí	
2.4.1. qCStatement OID	0.4.0.1862.1.1	Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.15096.1.3.1.42	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCPX-2	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal de xifrat de classe 2. Vegeu https://www.catcert.net/verCPX-2	Sí	
2.6. Subject Alternate Names		Sí	
2.6.1. rfc822Name	Correu electrònic del subscriptor del certificat	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	ec_al@catcert.net	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Present	Sí	
2.8.2. clientAuth	Present	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	http://epscd.catcert.net/crl/ec-al.crl	Sí	
2.9.2. distributionPoint	http://epscd2.catcert.net/crl/ec-al.crl	Sí	
2.10. NetscapeCertType	SSL client S/MIME	Sí	

Camp	Contingut	Obligat	Crític
2.11. Authority Info Access		Sí	
2.11.1. Access Method	id-ad-ocsp	Sí	
2.11.2. Access Location	http://ocsp.catcert.net	Sí	

5. CPX-2 Col·lectiu 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	Si	
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)	De conformitat amb la Política General de Certificació	Sí	
1.6.2. Organization (O)	Nom legal del subscriptor – organització externa	Sí	
1.6.3. Organizational Unit (OU)	Departament/Unitat	NO	
1.6.4. Organizational Unit (OU)	Serveis Públics de Certificació CPX-2	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCPX-2 (c)03	Sí	
1.6.6. Surname	Cognoms del posseïdor de claus	Sí	
1.6.7. Given Name	Nom del posseïdor de claus	Sí	
1.6.8. Serial Number	Segons Política General de Certificació	Sí	
1.6.9. Common Name (CN)	"CPX-2 Col " + Nom del posseïdor	Sí	

Camp	Contingut	Obligat	Crític
	de claus en text lliure		
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			
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	No seleccionat “0”		
2.3.2. Non Repudiation	No seleccionat “0”		
2.3.3. Key Encipherment	Seleccionat “1”	Sí	
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. Qualified Certificate Statements		Sí	
2.4.1. qCStatement OID	0.4.0.1862.1.1	Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.15096.1.3.1.42	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCPX-2	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal de xifrat de classe 2. Vegeu https://www.catcert.net/verCPX-2	Sí	
2.6. Subject Alternate Names		Sí	
2.6.1. rfc822Name	Correu electrònic del posseïdor de claus	Sí	
2.6.2. Serial Number	NIF del subscriptor	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	ec_safp@catcert.net	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Present	Sí	
2.8.2. clientAuth	Present	Sí	

Camp	Contingut	Obligat	Crític
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	http://epscd.catcert.net/crl/ec-safp.crl	Sí	
2.9.2. distributionPoint	http://epscd2.catcert.net/crl/ec-safp.crl	Sí	
2.10. NetscapeCertType	SSL client S/MIME	Sí	
2.11. Authority Info Access		Sí	
2.11.1. Access Method	id-ad-ocsp	Sí	
2.11.2. Access Location	http://ocsp.catcert.net	Sí	

6. CPX-2 Col·lectiu 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)	De conformitat amb la Política General de Certificació	Sí	
1.6.2. Organization (O)	Nom legal del subscriptor – organització externa	Sí	
1.6.3. Organizational Unit (OU)	Departament/Unitat	NO	
1.6.4. Organizational Unit (OU)	Serveis Públics de Certificació CPX-2	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCPX-2 (c)03	Sí	
1.6.6. Surname	Cognoms del posseïdor de claus	Sí	
1.6.7. Given Name	Nom del posseïdor de claus	Sí	
1.6.8. Serial Number	Segons Política General de Certificació	Sí	
1.6.9. Common Name (CN)	"CPX-2 Col " + Nom del posseïdor de claus en text lliure	Sí	

Camp	Contingut	Obligat	Crític
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			
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	No seleccionat “0”		
2.3.2. Non Repudiation	No seleccionat “0”		
2.3.3. Key Encipherment	Seleccionat “1”	Sí	
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. Qualified Certificate Statements		Sí	
2.4.1. qCStatement OID	0.4.0.1862.1.1	Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.15096.1.3.1.42	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCPX-2	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal de xifrat de classe 2. Vegeu https://www.catcert.net/verCPX-2	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correu electrònic del posseïdor de claus	Sí	
2.6.2. Serial Number	NIF del subscriptor	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	ec_al@catcert.net	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Present	Sí	
2.8.2. clientAuth	Present	Sí	

Camp	Contingut	Obligat	Crític
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	http://epscd.catcert.net/crl/ec-al.crl	Sí	
2.9.2. distributionPoint	http://epscd2.catcert.net/crl/ec-al.crl	Sí	
2.10. NetscapeCertType	SSL client S/MIME	Sí	
2.11. Authority Info Access		Sí	
2.11.1. Access Method	id-ad-ocsp	Sí	
2.11.2. Access Location	http://ocsp.catcert.net	Sí	