Agència Catalana
de Certificació

Estructura del certificat idCAT

Referència: D1112 N-Perfil idCAT
Versió: 1.7
Data: 30/6/2008

Informació general

Control documental

Projecte:	Agència Catalana de Certificació
Entitat de destinació:	
Títol:	Estructura del certificat idCAT
Codi de referència:	
Versió:	1.7
Data:	30/06/2008
Fitxer:	D1112 N-Perfil idCAT v1r7.doc
Eina/es d'edició:	Word 2002
Autor/s:	Àrea d'Assessorament i Recerca
Resum:	

Drets d'ús

Estat formal

Preparat per:	Revisat per:	Aprovat per:
Nom: Òscar Burgos Data: 2/06/2008	Nom: Data:	Nom: Data:

Control de versions

Versió	Data	Autor(s)	Gestió de la Qualitat	Canvis/Comentaris
1.0	8/10/2003	Alamillo	Oliveras	Creació del document
1.1	20/12/2003	Alamillo	Oliveras	Adaptació a Llei 59/2003
1.2	3/12/2004	Alamillo	Oliveras	Ampliació durada certificats
1.3	16/03/2006	Bonet	Odena	Modificació del camp “Serial Number” del Subject.
1.4	17/09/2007	AIR		Correcció nom idCAT
1.5	15/10/2007	ISIGMA		Format unificat
1.6	2/06/2008	Burgos		Revisió general del perfil i adaptació per a ús d’identificador de dispositiu i titular de dispositiu al Subject Alt. Name.

Índex

1. Certificat idCAT

Camp	Contingut	Obligatori	Crític
1. X.509 Field			
1.1. Versión	v3	SÍ	
1.2. Serial Number	Establert automàticament per la CA	SÍ	
1.3. Signature Algorithm	SHA-1 amb RSA	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	Passatge de la Concepció 11 08080 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)	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)	De conformitat amb la Política General de Certificació	Sí	
1.6.2. Organizational Unit (OU)	Vegeu https://www.catcert.net/verIdCAT (c) 05	Sí	
1.6.3. Surname	Cognoms del subscriptor del certificat	Sí	
1.6.4. GivenName	Nom de pila del subscriptor del certificat	Sí	
1.6.5. SerialNumber	Segons Política General de Certificació	Sí	
1.6.6. CommonName (CN)	Identitat del subscriptor del certificat en text lliure	Sí	
1.7. Subject Public Key Info	1024-Bit clau pública codificat d’acord amb RFC2459 & PKCS#1	Sí	
2. X.509v3 Extensions			
2.1. Authority Key Identifier	Present	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			

Camp	Contingut	Obligatori	Crític
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" (només per certificats amb xifrat)	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	1.3.6.1.4.1.15096.1.3.1.84.1 (sense xifrat) 1.3.6.1.4.1.15096.1.3.1.86.1 (amb xifrat)	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/veridCAT	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal idCAT, reconegut d'identificació, signatura i xifrat (opcional) de classe 2 individual. Vegeu https://www.catcert.net/veridCAT	Sí	
2.6. Subject Alternative Name		Sí	
2.6.1. rfc822Name	usuari@domini.ext	Sí	
2.6.2. DN			
2.6.2.1. Country (C)	ES		
2.6.2.2. Organitzation Name	Agència Catalana de Certificació		
2.6.2.3. Organizational Unit (OU)	IDCAT		
2.6.2.4. Serial Number	Identificació numèrica alternativa per identificar el certificat i/o el subscriptor		
2.6.2.5. Common Name (CN)	Identitat del subscriptor del certificat en text lliure		
2.6.3. Other Name			
2.6.3.1. 1.3.6.1.4.1.1509	Identificador del model de dispositiu on s'allotja el certificat, en text		

Camp	Contingut	Obligatori	Crític
6.1.1.1 (DeviceModelID)	lliure.		
2.6.4. Other Name			
2.6.4.1. 1.3.6.1.4.1.1509 6.1.1.2 (DeviceHolderID)	Identitat del titular del dispositiu on s'allotja el certificat, en text lliure.		
2.7. Issuer Alternative Name			
2.7.1. rfc822Name	ec_idCAT@catcert.net	Sí	
2.8. Extended Key Usage			
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-idCAT.crl	Sí	
2.9.2. distributionPoint	http://epscd2.catcert.net/crl/ec-idCAT.crl	Sí	
2.10. Subject Directory Attributes		Sí	
2.10.1. countryOfCitizenship	Estat on té la nacionalitat el subscriptor.	Sí	
2.10.2. countryOfResidence	Estat on té la residència el subscriptor.	Sí	
2.11. NetscapeCertType	SSL client, SMIME client	Sí	
2.12. Authority Info Access		Sí	
2.12.1. Access Method	id-ad-ocsp	Sí	
2.12.2. Access Location	http://ocsp.catcert.net	Sí	

2. Perfil d'exemple IdCAT persona física (subtipus de CPISA-2)

Camp	Contingut	Obligatori	Crític
1. X.509v1 Field			
1.1. Versión	v3	SÍ	
1.2. Serial Number	Establert automàticament per la CA	SÍ	
1.3. Signature Algorithm	SHA-1 amb RSA	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	Passatge de la Concepció 11 08080 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)	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)	De conformitat amb la Política General de Certificació	SÍ	
1.6.2. Organizational Unit (OU)	Vegeu https://www.catcert.net/verIdCAT (c) 03	SÍ	
1.6.3. Surname	Cognoms del subscriptor del certificat	SÍ	
1.6.4. GivenName	Nom de pila del subscriptor del certificat	SÍ	
1.6.5. SerialNumber	Segons Política General de Certificació	SÍ	

Camp	Contingut	Obligatori	Crític
1.6.6. CommonName (CN)	Identitat del subscriptor del certificat en text lliure	Sí	
1.7. Subject Public Key Info	1024-Bit clau pública codificat d'acord amb 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	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. 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	1.3.6.1.4.1.15096.1.3.1.84.1	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verIdCAT	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal idCAT, reconegut d'identificació i signatura de classe 2 individual. Vegeu https://www.catcert.net/verIdCAT	Sí	
2.6. Subject Alternative Name		Sí	
2.6.1. rfc822Name	usuari@domini.ext	Sí	
2.6.2. DN			

Camp	Contingut	Obligatori	Crític
2.6.2.1. Country (C)	ES		
2.6.2.2. Organitzation Name	Agència Catalana de Certificació		
2.6.2.3. Organizational Unit (OU)	IDCAT		
2.6.2.4. Serial Number	Número de sèrie del certificat, establert automàticament per la CA.		
2.6.2.5. Common Name (CN)	Identitat del subscriptor del certificat en text lliure		
2.6.3. Other Name			
2.6.3.1. 1.3.6.1.4.1.15096. 1.1.1 (DeviceModelID)	Gemalto FullMultimedia SIM		
2.6.4. Other Name			
2.6.4.1. 1.3.6.1.4.1.15096. 1.1.2 (DeviceHolderID)	Vodafone		
2.7. Issuer Alternative Name			
2.7.1. rfc822Name	ec_idCAT@catcert.net	Sí	
2.8. Extended Key Usage			
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-idCAT.crl	Sí	
2.9.2. distributionPoint	http://epscd2.catcert.net/crl/ec-idCAT.crl	Sí	
2.10. Subject Directory Attributes		Sí	
2.10.1. countryOfCitizenship	Estat on té la nacionalitat el subscriptor.	Sí	
2.10.2. countryOfResidence	Estat on té la residència el subscriptor.	Sí	
2.11. NetscapeCertType	SSL client, SMIME client	Sí	
2.12. Authority Info Access		Sí	
2.12.1. Access Method	id-ad-ocsp	Sí	
2.12.2. Access Location	http://ocsp.catcert.net	Sí	

3. Perfil d'exemple IdCAT persona física (subtipus de CPIXSA-2)

Camp	Contingut	Obligatori	Crític
1. X.509v1 Field			
1.1. Versión	v3	SÍ	
1.2. Serial Number	Establert automàticament per la CA	SÍ	
1.3. Signature Algorithm	SHA-1 amb RSA	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	Passatge de la Concepció 11 08080 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)	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)	De conformitat amb la Política General de Certificació	Sí	
1.6.2. Organizational Unit (OU)	Vegeu https://www.catcert.net/verIdCATX (c) 03	Sí	
1.6.3. Surname	Cognoms del subscriptor del certificat	Sí	
1.6.4. GivenName	Nom de pila del subscriptor del certificat	Sí	
1.6.5. SerialNumber	Segons Política General de	Sí	

Camp	Contingut	Obligatori	Crític
	Certificació		
1.6.6. CommonName (CN)	Identitat del subscriptor del certificat en text lliure	Sí	
1.7. Subject Public Key Info	1024-Bit clau pública codificat d'acord amb 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	Seleccionat "1"	Sí	
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	1.3.6.1.4.1.15096.1.3.1.86.1	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verIdCATX	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal IDCAT, reconegut d'identificació, signatura i xifrat de classe 2 individual. Vegeu https://www.catcert.net/verIdCATX	Sí	
2.6. Subject Alternative Name		Sí	
2.6.1. rfc822Name	usuari@domini.ext	Sí	

Camp	Contingut	Obligatori	Crític
2.6.2. DN			
2.6.2.1. Country (C)	ES		
2.6.2.2. Organitzation Name	Agència Catalana de Certificació		
2.6.2.3. Organizational Unit (OU)	IDCAT		
2.6.2.4. Serial Number	Número de sèrie del certificat, establert automàticament per la CA.		
2.6.2.5. Common Name (CN)	Identitat del subscriptor del certificat en text lliure		
2.6.3. Other Name			
2.6.3.1. 1.3.6.1.4.1.15096.1.1.1 (DeviceModelID)	Clauer idCAT		
2.6.4. Other Name			
2.6.4.1. 1.3.6.1.4.1.15096.1.1.2 (DeviceHolderID)	Ajuntament de Sant Feliu de Llobregat		
2.7. Issuer Alternative Name			
2.7.1. rfc822Name	ec_idCAT@catcert.net	Sí	
2.8. Extended Key Usage			
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-idCAT.crl	Sí	
2.9.2. distributionPoint	http://epscd2.catcert.net/crl/ec-idCAT.crl	Sí	
2.10. Subject Directory Attributes		Sí	
2.10.1. countryOfCitizenship	Estat on té la nacionalitat el subscriptor.	Sí	
2.10.2. countryOfResidence	Estat on té la residència el subscriptor.	Sí	
2.11. NetscapeCertType	SSL client, SMIME client	Sí	
2.12. Authority Info Access		Sí	
2.12.1. Access Method	id-ad-ocsp	Sí	
2.12.2. Access Location	http://ocsp.catcert.net	Sí	