Agència Catalana de Certificació

Estructura dels certificats CDS-1 Seu electrònica (nivells alt i mig)

Referència:	D1112 N-Perfil CDS-1 Seu electrònica
Versió:	1.10
Data:	12/11/2008

Agència Catalana de Certificació

Informació general

Control documental

Projecte:	Agència Catalana de Certificació
Entitat de destinació:	
Títol:	Estructura dels certificats CDS-1 Seu electrònica (nivells mig i alt).
Codi de referència:	
Versió:	1.10
Data:	12/11/2008
Fitxer:	D1112 N-Perfil CDS-1 Seu electrònica EV v1r10.doc
Eina/es d'edició:	Word 2007
Autor/s:	Alamillo Domingo, Ignacio; Henao Hoyos, Erika López González, Chema; Cruellas Ibarz, Marta
Resum:	

Drets d'ús

Estat formal

Preparat per:	Revisat per:	Aprovat per:
Nom: isigma Data: 02/03/2008	Nom: Àrea d'AiR Data: 12/11/2008	Nom: Data:

Control de versions

Versió	Data	Autor(s)	Gestió de la Qualitat	Canvis/Comentaris
1.0	04/02/2008	isigma		Creació del document
1.1	18/02/2008	isigma		Afegit CPISR i canvis proposats per CATCert a CSgE i CSeE
1.2	21/02/2008	isigma		Canvis proposats per CATCert a CPISR
1.3	02/03/2008	isigma		Canvis proposats per CATCert a CPSvAP (anterior CPISR)
1.4	10/03/2008	isigma		Addició de extensions de qc a certificats de Seu i de Segell
1.5	25/03/2008	Henao		Correcció final del document
1.6	08/04/2008	Henao		Document independent per als CDS-1 Seu electrònica
1.7	14/04/2008	Cruellas		Addició camps conforme a EV (CA/Browser forum)
1.8	22/04/2008	Cruellas		Esmena QcEuRetentionPeriod
1.9	22/05/2008	Cruellas		Revisió conforme a modificacions en els perfils de referència del MAP
1.10	12/11/2008	Cruellas		S'afegeix un 2n "dnsName" dins del "Subject Alternate Names" (2.6.2.) per suportar certificats multidomini.

Índex

1. CDS-1 Seu electrònica de nivell alt

Certificat de dispositiu servidor segur, de Seu Electrònica, d'acord amb la Llei 11/2007, de 22 de juny, d'Accés Electrònic dels Ciutadans als Serveis Públics i nivell alt. Certificat basat en la política bàsica CDS.

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	Certificats emesos fins al 31/12/2010: SHA-1 with RSA Signature Certificats emesos després del 31/12/2010: SHA-256[1]	Sí	
1.4. Issuer Distinguished Name	Segons cada EC	Sí	
1.5. Validity	1 any	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)	denominació legal de l'Administració Pública, òrgan o entitat administrativa	Sí	
1.6.3. Organizational Unit (OU)	Identificació de la seu electrònica	NO	
1.6.4. Organizational Unit (OU)	"Serveis Públics de Certificació CDS-1 Seu electrònica"	Sí	
1.6.5. Organizational Unit (OU)	"Vegeu https://www.catcert.net/verCDS-1 Seu (c)08"	Sí	
1.6.6. Common Name (CN)	Adreça IP o DNS del servidor[2]	Sí	
1.6.7. Bussiness Category	[OID: joint-iso-itu.2.5.4.15] Ha de contenir un dels següents strings: a) "V1.0, Clause 5.(b)" quan el titular sigui una organització privada (*Private organization*).	Sí	

[1] SHA-1 s'hauria d'emprar només fins que SHA-256 estigui suportat pels navegadors àmpliament emprats per la comunitat d'usuaris.

[2] No es permet identificar múltiples subdominis amb un únic certificat (posant, per exemple: *.catcert.cat)

Camp	Contingut	Obligat	Crític
	b) "V1.0, Clause 5.(c)" quan el titular sigui un ens públic (*Government entity*). c) "V1.0, Clause 5.(d)" quan el titular sigui una empresa (*Bussiness entity*).		
1.6.8. JurisdictionOfIncorporation LocalityName	[OID: 1.3.6.1.4.1.311.60.2.1.1] Jurisdicció: Localitat en la que està registrat l'ens/empresa (si cal)	No	
1.6.9. JurisdictionOfIncorporation StateOrProvinceName	[OID: 1.3.6.1.4.1.311.60.2.1.2] Jurisdicció: Província en la que està registrat l'ens/empresa (si cal)	No	
1.6.10. JurisdictionOfIncorporation CountryName	[OID: 1.3.6.1.4.1.311.60.2.1.3] Jurisdicció: País en el que està registrat l'ens/empresa	Sí	
1.6.11. SerialNumber	[OID: joint-iso-itu.2.5.4.5] CIF de l'ens/empresa	Sí	
1.6.12. StreetAddress	[OID: joint-iso-itu.2.5.4.9] Adreça postal de l'ens	No	
1.6.13. LocalityName	[OID: joint-iso-itu.2.5.4.7] Localitat	Sí	
1.6.14. StateOrProvinceName	[OID: joint-iso-itu.2.5.4.8] Província	Sí	
1.6.15. CountryName	[OID: joint-iso-itu.2.5.4.6] País	Sí	
1.6.16. PostalCode	[OID: joint-iso-itu.2.5.4.17] Codi postal	No	
1.7. Subject Public Key Info	2048-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	Seleccionat "1"	Sí	
2.3.2. Content Commitment	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"		

Camp	Contingut	Obligat	Crític
2.3.7. CRL Signature	No seleccionat "0"		
2.4. Qualified Certificate Statements		Sí	
2.4.1. QcCompliance	OID 0.4.0.1862.1.1	Sí	
2.4.2. QcEuRetentionPeriod	OID 0.4.0.1862.1.3	Sí	
2.4.2.1. QcEuRetentionPeriod	15 anys.	Sí	
2.4.3. QcSSCD	OID 0.4.0.1862.1.4	Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	CATCert.1.3.1.51.3	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCDS-1 Seu	Sí	
2.5.2.2. User Notice	"Aquest és un certificat reconegut de seu electrònica amb conformitat amb la llei 11/2007 i amb l'especificació EV, de classe 1 i nivell alt. Vegeu https://www.catcert.net/verCDS-1 Seu"	Sí	
2.6. Subject Alternate Names		Sí	
2.6.1. rfc822Name	adreça de correu-e per a la formulació de suggeriments i queixes[3]	Sí	
2.6.2. dnsName	Nom de Domini DNS de la seu	NO[4]	
2.6.3. dnsName	Nom de Domini DNS alternatiu de la seu	NO[5]	
2.6.4. Directory Name	Identitat Administrativa	Sí	
2.6.4.1. Tipus de certificat	"Certificat de seu electrònica, de classe 1, nivell alt" OID: 1.3.6.1.4.1.14862.1.4.2.1.1	Sí	
2.6.4.2. Nom de l'entitat subscriptora	L'entitat propietària del certificat OID: 1.3.6.1.4.1.14862.1.4.2.1.2	Sí	

[3] segons es requereix a l'article 10.3 de la llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics

[4] El contingut d'aquest camp ha de coincidir amb l'especificat al "CommonName" del "Subject" (1.6.6.). Per exemple:
1.6.6. CN: catcert.net
2.6.2. dnsName: catcert.net

[5] Per a certificats multidomini caldrà que aquest 2n "dnsName" (2.6.3.) contingui el nom de domini DNS alternatiu. Per exemple:
2.6.3. dnsName: catcert.cat

Camp	Contingut	Obligat	Crític
2.6.4.3. NIF de l'entitat subscriptora	NIF de l'entitat subscriptora OID: 1.3.6.1.4.1.14862.1.4.2.1.3	Sí	
2.6.4.4. Nom descriptiu de la seu electrònica	Breu descripció de la seu indicant el seu nom OID: 1.3.6.1.4.1.14862.1.4.2.1.4	Sí	
2.6.4.5. Denominació de nom de domini IP	Domini al que pertany la seu[6] OID: 1.3.6.1.4.1.14862.1.4.2.1.5	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	ec-xxx@catcert.net	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. serverAuth	Present	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	http://epscd.catcert.net/crl/ec-xxx.crl	Sí	
2.9.2. distributionPoint	http://epscd2.catcert.net/crl/ec-xxx.crl	Sí	
2.10. Authority Info Access		Sí	
2.10.1. Access Method	Id-ad-ocsp	Sí	
2.10.2. Acces Location	http://ocsp.catcert.net	Sí	

[6] El contingut d'aquest camp ha de coincidir amb el del "Common Name" del "Subject" (1.6.6.).

2. CDS-1 Seu electrònica de nivell mig

Certificat de dispositiu servidor segur, de Seu Electrònica, d'acord amb la Llei 11/2007, de 22 de juny, d'Accés Electrònic dels Ciutadans als Serveis Públics i nivell mig. Certificat basat en la política bàsica CDS.

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	Certificats emesos fins al 31/12/2010: SHA-1 with RSA Signature Certificats emesos després del 31/12/2010: SHA-256[7]	Sí	
1.4. Issuer Distinguished Name	Segons cada EC	Sí	
1.5. Validity	1 any Els certificats amb claus de 1024 bits han de caducar no més tard del 31/12/2010.	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)	denominació legal de l'Administració Pública, òrgan o entitat administrativa	Sí	
1.6.3. Organizational Unit (OU)	Identificació de la seu electrònica	NO	
1.6.4. Organizational Unit (OU)	"Serveis Públics de Certificació CDS-1 Seu electrònica"	Sí	
1.6.5. Organizational Unit (OU)	"Vegeu https://www.catcert.net/verCDS-1 Seu (c)08"	Sí	
1.6.6. Common Name (CN)	Adreça IP o DNS del servidor[8]	Sí	
1.6.7. Bussiness Category	[OID: joint-iso-itu.2.5.4.15] Ha de contenir un dels següents strings: d) "V1.0, Clause 5.(b)" quan el titular sigui una	Sí	

[7] SHA-1 s'hauria d'emprar només fins que SHA-256 estigui suportat pels navegadors àmpliament emprats per la comunitat d'usuaris.

[8] No es permet identificar múltiples subdominis amb un únic certificat (posant, per exemple: *.catcert.cat)

Camp	Contingut	Obligat	Crític
	organització privada (*Private organization*). e) "V1.0, Clause 5.(c)" quan el titular sigui un ens públic (*Government entity*). f) "V1.0, Clause 5.(d)" quan el titular sigui una empresa (*Bussiness entity*).		
1.6.8. JurisdictionOfIncorporationLocalityName	[OID: 1.3.6.1.4.1.311.60.2.1.1] Jurisdicció: Localitat en la que està registrat l'ens/empresa (si cal)	No	
1.6.9. JurisdictionOfIncorporationStateOrProvinceName	[OID: 1.3.6.1.4.1.311.60.2.1.2] Jurisdicció: Província en la que està registrat l'ens/empresa (si cal)	No	
1.6.10. JurisdictionOfIncorporationCountryName	[OID: 1.3.6.1.4.1.311.60.2.1.3] Jurisdicció: País en el que està registrat l'ens/empresa	Sí	
1.6.11. SerialNumber	[OID: joint-iso-itu.2.5.4.5] CIF de l'ens/empresa	Sí	
1.6.12. StreetAddress	[OID: joint-iso-itu.2.5.4.9] Adreça postal de l'ens	No	
1.6.13. LocalityName	[OID: joint-iso-itu.2.5.4.7] Localitat	Sí	
1.6.14. StateOrProvinceName	[OID: joint-iso-itu.2.5.4.8] Província	Sí	
1.6.15. CountryName	[OID: joint-iso-itu.2.5.4.6] País	Sí	
1.6.16. PostalCode	[OID: joint-iso-itu.2.5.4.17] Codi postal	No	
1.7. Subject Public Key Info	1024 o 2048-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	Seleccionat "1"	Sí	
2.3.2. Content Commitment	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"		

Camp	Contingut	Obligat	Crític
2.3.7. CRL Signature	No seleccionat "0"		
2.4. Qualified Certificate Statements		Sí	
2.4.1. QcCompliance	OID 0.4.0.1862.1.1	Sí	
2.4.2. QcEuRetentionPeriod	OID 0.4.0.1862.1.3	Sí	
2.4.2.1. QcEuRetention Period	15 anys.	Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	CATCert.1.3.1.51.2	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCDS-1 Seu	Sí	
2.5.2.2. User Notice	"Aquest és un certificat reconegut de seu electrònica amb conformitat amb la llei 11/2007 i amb l'especificació EV, de classe 1 i nivell mig. Vegeu https://www.catcert.net/verCDS-1 Seu"	Sí	
2.6. Subject Alternate Names		Sí	
2.6.1. rfc822Name	adreça de correu-e per a la formulació de suggeriments i queixes[9]	Sí	
2.6.2. dnsName	Nom de Domini DNS de la seu	No[10]	
2.6.3. dnsName	Nom de Domini DNS de la seu	No[11]	
2.6.4. Directory Name	Identitat Administrativa	Sí	
2.6.4.1. Tipus de certificat	Certificat de seu electrònica, de classe 1, nivell mig OID: 1.3.6.1.4.1.14862.1.4.2.2.1	Sí	
2.6.4.2. Nom de l'entitat subscriptora	L'entitat propietària del certificat OID: 1.3.6.1.4.1.14862.1.4.2.2.2	Sí	
2.6.4.3. NIF de l'entitat subscriptora	NIF de l'entitat subscriptora OID: 1.3.6.1.4.1.14862.1.4.2.2.3	Sí	
2.6.4.4. Nom descriptiu	Breu descripció de la seu indicant el seu nom	Sí	

[9] segons es requereix a l'article 10.3 de la llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics

[10] El contingut d'aquest camp ha de coincidir amb l'especificat al "CommonName" del "Subject" (1.6.6.). Per exemple:
1.6.6. CN: catcert.net
2.6.2. dnsName: catcert.net

[11] Per a certificats multidomini caldrà que aquest 2n "dnsName" (2.6.3.) contingui el nom de domini DNS alternatiu. Per exemple:
2.6.3. dnsName: catcert.cat

Camp	Contingut	Obligat	Crític
de la seu electrònica	OID: 1.3.6.1.4.1.14862.1.4.2.2.4		
2.6.4.5. Denominació de nom de domini IP	Domini al que pertany la seu[12] OID: 1.3.6.1.4.1.14862.1.4.2.2.5	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	ec-xxx@catcert.net	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. serverAuth	Present	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	http://epscd.catcert.net/crl/ec-xxx.crl	Sí	
2.9.2. distributionPoint	http://epscd2.catcert.net/crl/ec-xxx.crl	Sí	
2.10. Authority Info Access		Sí	
2.10.1. Access Method	Id-ad-ocsp	Sí	
2.10.2. Acces Location	http://ocsp.catcert.net	Sí	

[12] El contingut d'aquest camp ha de coincidir amb el del "Common Name" del "Subject" (1.6.6.).