



Agència Catalana
de Certificació

Estructura del certificat CPISR amb Càrrec per a Ús Concret

Referència: D1112 N-Perfil CPISR Càrrec Ús
Versió: 1.3
Data: 15/10/2007

Informació general

Control documental

Projecte: Agència Catalana de Certificació

Entitat de destinació:

Títol: Estructura del certificat CPISR amb Càrrec per a Ús Concret

Codi de referència:

Versió: 1.3

Data: 17/10/2007

Fitxer: D1112 N-Perfil CPISR Càrrec Ús v1r3 Final

Eina/es d'edició: Word 2002

Autor/s: Alamillo Domingo, Ignacio

Resum:

Drets d'ús

La present documentació és propietat de l'AGÈNCIA CATALANA DE CERTIFICACIÓ, és confidencial i no podrà ésser objecte de reproducció total o parcial, tractament informàtic ni transmissió de cap forma o per qualsevol mitjà, ja sigui electrònic, mecànic, per fotocòpia, registre o qualsevol altre. Tanmateix, tampoc no podrà ésser objecte de préstec, lloguer o qualsevol forma de cessió d'ús sense el consentiment previ i per escrit de l'AGÈNCIA CATALANA DE CERTIFICACIÓ, titular del dret d'autor (copyright). L'incompliment de les limitacions assenyalades per qualsevol persona que tingui accés a la documentació serà perseguida d'acord amb la llei.

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	12/05/2005	Alamillo	Oliveras	Creació del document
1.1	15/03/2006	Bonet	Odena	Modificació dels camps "rfc822Name" i "Serial Number" del Subject.
1.2	17/09/2007	AIR		Camp OU com opcional
1.3	15/10/2007	ISIGMA		Afegit ús de clau "ContentCommitment" (antic "NonRepudiation")

Índex

<i>Estructura del certificat CPISR amb Càrrec per a Ús Concret</i>	1
<i>Informació general</i>	2
Control documental	2
Drets d'ús	2
Estat formal.....	2
Control de versions	3
<i>Índex</i>	4
1. <i>CPISR-1 amb Càrrec Ús EC-SAFP</i>	5
2. <i>CPISR-1 amb Càrrec Ús EC-AL</i>	8
3. <i>CPISR-1 amb Càrrec Ús EC-UR</i>	11
4. <i>CPISR-1 amb Càrrec Ús EC-Parlament</i>	14
5. <i>CPISR-1 amb Càrrec Ús EC-URV</i>	17

1. CPISR-1 amb Càrrec Ús 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 CPISR-1 amb càrrec ús concret	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCPISR-1CàrrecUsSAFP(c)03	Sí	
1.6.6. Organizational Unit (OU)	Ús concret previst	Sí	
1.6.7. Surname	Cognoms del posseïdor de claus	Sí	
1.6.8. Given Name	Nom del posseïdor de claus	Sí	

Estructura del certificat CPISR amb Càrrec per a Ús Concret

Camp	Contingut	Obligat	Crític
1.6.9. Title	Categoria i/o càrrec del posseïdor de claus	Sí	
1.6.10. Serial Number	Segons Política General de Certificació	Sí	
1.6.11. Common Name (CN)	"CPISR-1 CU " + nom del posseïdor de claus 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			
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	Seleccionat "1"	Sí	
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	1.3.6.1.4.1.15096.1.3.1.81.3.1	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCPISR-1CàrrecUsSAFP	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal reconegut d'identificació i signatura reconeguda de classe 1 amb càrrec per a ús concret. Vegeu https://www.catcert.net/verCPISR-1CàrrecUsSAFP	Sí	
2.6. Subject Alternate Names		Sí	

**Estructura del certificat CPISR amb
Càrrec per a Ús Concret**

Camp	Contingut	Obligat	Crític
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	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	http://epsd.catcert.net/crl/ec-safp.crl	Sí	
2.9.2. distributionPoint	http://epsd2.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. CPISR-1 amb Càrrec Ús 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 CPISR-1 amb càrrec ús concret	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCPISR-1CàrrecUsAL (c)03	Sí	
1.6.6. Organizational Unit (OU)	Ús concret previst	Sí	
1.6.7. Surname	Cognoms del posseïdor de claus	Sí	
1.6.8. Given Name	Nom del posseïdor de claus	Sí	

Estructura del certificat CPISR amb Càrrec per a Ús Concret

Camp	Contingut	Obligat	Crític
1.6.9. Title	Categoria i/o càrrec del posseïdor de claus	Sí	
1.6.10. Serial Number	Segons Política General de Certificació	Sí	
1.6.11. Common Name (CN)	"CPISR-1 CU " + nom del posseïdor de claus 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			
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	Seleccionat "1"	Sí	
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	1.3.6.1.4.1.15096.1.3.1.81.3.2	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCPISR-1CàrrecUsAL	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal reconegut d'identificació i signatura reconeguda de classe 1 amb càrrec per a ús concret. Vegeu https://www.catcert.net/verCPISR-1CàrrecUsAL	Sí	
2.6. Subject Alternate Names		Sí	

**Estructura del certificat CPISR amb
Càrrec per a Ús Concret**

Camp	Contingut	Obligat	Crític
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	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	http://epsd.catcert.net/crl/ec-al.crl	Sí	
2.9.2. distributionPoint	http://epsd2.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. CPISR-1 amb Càrrec Ús 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)	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 CPISR-1 amb càrrec ús concret	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCPISR-1CàrrecUsUR(c)03	Sí	
1.6.6. Organizational Unit (OU)	Ús concret previst	Sí	
1.6.7. Surname	Cognoms del posseïdor de claus	Sí	
1.6.8. Given Name	Nom del posseïdor de claus	Sí	

Estructura del certificat CPISR amb Càrrec per a Ús Concret

Camp	Contingut	Obligat	Crític
1.6.9. Title	Categoria i càrrec del posseïdor de claus	Sí	
1.6.10. Serial Number	Segons Política General de Certificació	Sí	
1.6.11. Common Name (CN)	"CPISR-1 CU " + nom del posseïdor de claus 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			
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	Seleccionat "1"	Sí	
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	1.3.6.1.4.1.15096.1.3.1.81.3.3	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCPISR-1CàrrecUsUR	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal reconegut d'identificació i signatura reconeguda de classe 1 amb càrrec per a ús concret. Vegeu https://www.catcert.net/verCPISR-1CàrrecUsUR	Sí	
2.6. Subject Alternate Names		Sí	

**Estructura del certificat CPISR amb
Càrrec per a Ús Concret**

Camp	Contingut	Obligat	Crític
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_ur@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://epsd.catcert.net/crl/ec-ur.crl	Sí	
2.9.2. distributionPoint	http://epsd2.catcert.net/crl/ec-ur.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	

4. CPISR-1 amb Càrrec Ús 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 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 CPISR-1 amb càrrec	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCPISR-1CàrrecUsParlament(c)04	Sí	
1.6.6. Organizational Unit (OU)	Ús concret previst	Sí	
1.6.7. Surname	Cognoms del posseïdor de claus	Sí	
1.6.8. Given Name	Nom del posseïdor de claus	Sí	

Estructura del certificat CPISR amb Càrrec per a Ús Concret

Camp	Contingut	Obligat	Crític
1.6.9. Title	Categoria i/o càrrec del posseïdor de claus	Sí	
1.6.10. Serial Number	Segons Política General de Certificació	Sí	
1.6.11. Common Name (CN)	"CPISR-1 CU " + nom del posseïdor de claus 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			
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	Seleccionat "1"	Sí	
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	1.3.6.1.4.1.15096.1.3.1.81.3.4	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCPISR-1CàrrecUsParlament	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal reconegut d'identificació i signatura reconeguda de classe 1 amb càrrec per a ús concret. Vegeu https://www.catcert.net/verCPISR-1CàrrecUsParlament	Sí	
2.6. Subject Alternate Names		Sí	

Estructura del certificat CPISR amb Càrrec per a Ús Concret

Camp	Contingut	Obligat	Crític
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_parlament@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://epsd.catcert.net/crl/ec-parlament.crl	Sí	
2.9.2. distributionPoint	http://epsd2.catcert.net/crl/ec-parlament.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	

5. CPISR-1 amb Càrrec Ús 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)	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 CPISR-1 amb càrrec	Sí	
1.6.5. Organizational Unit (OU)	Vegeu https://www.catcert.net/verCPISR-1CàrrecUsURV(c)05	Sí	
1.6.6. Organizational Unit (OU)	Ús concret previst	Sí	
1.6.7. Surname	Cognoms del posseïdor de claus	Sí	
1.6.8. Given Name	Nom del posseïdor de claus	Sí	

Estructura del certificat CPISR amb Càrrec per a Ús Concret

Camp	Contingut	Obligat	Crític
1.6.9. Title	Categoria i càrrec del posseïdor de claus	Sí	
1.6.10. Serial Number	Segons Política General de Certificació	Sí	
1.6.11. Common Name (CN)	"CPISR-1 CU " + nom del posseïdor de claus 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			
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	Seleccionat "1"	Sí	
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	1.3.6.1.4.1.15096.1.3.1.81.3.5	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	https://www.catcert.net/verCPISR-1CàrrecUsURV	Sí	
2.5.2.2. User Notice	Aquest és un certificat personal reconegut d'identificació i signatura reconeguda de classe 1 amb càrrec per a ús concret. Vegeu https://www.catcert.net/verCPISR-1CàrrecUsURV	Sí	
2.6. Subject Alternate Names		Sí	

Estructura del certificat CPISR amb Càrrec per a Ús Concret

Camp	Contingut	Obligat	Crític
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_urv@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://epsd.catcert.net/crl/ec-urv.crl	Sí	
2.9.2. distributionPoint	http://epsd2.catcert.net/crl/ec-urv.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	