



Consorci
Administració Oberta
de Catalunya

Descripció del Perfil de certificats CPISR-1 Càrrec opcional

 Generalitat
de Catalunya

LOCALRET

Control documental

| | | |
|--------------------------------|--|---|
| Estat formal | Elaborat per: Chema López | Aprovat per: Francesc Ferrer |
| Data de creació | 23/02/2010 | |
| Control de versions | Versió | 2.6 |
| | Data: | 1/20/16 |
| | Descripció: | Consolidació de totes les variants del perfil CPISR-1 en un de sol. |
| Nivell accés informació | Pública | |
| Títol | Descripció del Perfil de certificats CPISR-1 Càrrec opcional | |
| Fitxer | D1112 N-Perfil EC-SectorPublic CPISR-1 Càrrec opcional v2r6.doc | |
| Control de còpies | Només les còpies disponibles a la web del Consorci AOC a https://www.aoc.cat/CATCert/Regulacio garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades. | |
| Drets d'autor | Aquesta obra està subjecta a una llicència Reconeixement-No comercial-Sense obres derivades 2.5 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA. | |

Índex

| | | |
|---|---|---|
| 1 | Descripció del perfil CPISR-1 C de l'EC-SectorPublic..... | 4 |
|---|---|---|

Descripció del perfil CPISR-1 C de l'EC-SectorPublic

| Camp | Descripció Contingut | Valor | Obligat |
|---------------------------------|--|--|---------|
| 1. X.509 Field | | | |
| 1.1. Version | v3 | 2 | Sí |
| 1.2. Serial Number | <i>Integer positiu, establert automàticament per l'EC, que identificarà de manera unívoca el certificat.</i> | | Sí |
| 1.3. Signature Algorithm | | | Sí |
| 1.3.1. Identifier | | 1.2.840.113549.1.1.5 | Sí |
| 1.3.2. Description | | "SHA-1 with RSA Signature" | Sí |
| 1.4. Issuer Distinguished Name | <i>Establert automàticament per l'EC.</i> | | Sí |
| 1.4.1. Common Name (CN) | | "EC-SectorPublic" | Sí |
| 1.4.2. Country (C) | | "ES" | Sí |
| 1.4.3. Organization (O) | | "CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA" | Sí |
| 1.4.4. Organizational Unit (OU) | | "Serveis Públics de Certificació" | Sí |
| 1.5. Validity | | Fins a 5 anys | Sí |
| 1.5.1. Not Before | <i>e.g., "00:00:01 01 September 1999"</i> | | Sí |
| 1.5.2. Not After | <i>e.g., "23:59:59 31 August 2003"</i> | | Sí |

| Camp | Descripció Contingut | Valor | Obligat |
|-------------------------|--|--|---------|
| 1.6. Subject | <i>Tots aquests camps es codificaran amb UTF-8</i> | | Sí |
| 1.6.1. Common Name (CN) | <i>OID: 2.5.4.3</i> | <i>"CPISR-1 C " + Nom i cognoms del posseïdor de claus</i> | Sí |
| 1.6.2. Given Name (G) | <i>OID: 2.5.4.42</i> | <i>Nom de pila del posseïdor de claus, conforme al document identificatiu.</i> | Sí |
| 1.6.3. Surname (SN) | <i>OID: 2.5.4.4</i> | <i>Cognoms del posseïdor de claus, conforme al document identificatiu.</i> | Sí |
| 1.6.4. Serial Number | <i>OID: 2.5.4.5</i> | <i>A) Número del document identificatiu (NIF/NIE) del posseïdor de claus. O bé:</i> <i>B) Número del document nacional d'identitat del país d'origen/Passaport) del posseïdor de claus.¹</i> | Sí |

¹ Conforme a la Política general de certificació, apartat "Resolució de conflictes relatiu a noms": En **certificats corporatius**, els conflictes de noms dels posseïdors de claus que apareixen identificats amb el seu nom real se solucionen mitjançant la inclusió, en el nom distingit del certificat, de:

- En el cas que l'"Organization" del camp "Subject" (això és, l'ens subscriptor) estigui sotmesa a dret espanyol:
 - En el cas de posseïdors de claus nacionals espanyols, el número de DNI del subscriptor.
V.gr.: (C) = ES; (SN) = #DNI
 - En el cas d'estrangers amb algun tipus de vinculació amb Espanya, com ara la residència en territori espanyol, el n número de NIE del subscriptor.
V.gr.: francès (C) = ES; (SN) = #NIE
V.gr.: argentí (C) = ES; (SN) = #NIE
 - En el cas d'estrangers nacionals d'Estats que són part de l'Acord Schengen i que no disposen de NIE, el número de document nacional d'identitat del país d'origen o de procedència o passaport vigent del subscriptor. També es podrà consignar, abans del número del documento identificador citat, el codi del país del que el subscriptor és nacional, de conformitat amb els paràmetres establerts per la norma ISO 3166 Codes (Countries), separat per un guió.
V.gr.: italià (C) = IT; (SN) = #Documento nacional de identitat
V.gr.: italià (C) = IT; (SN) = IT-#Documento nacional de identitat
 - En el cas d'estrangers nacionals d'Estats que no són part de l'Acord Schengen i que no disposen de NIE, el número de passaport ordinari, diplomàtic, oficial o de servei, del subscriptor vàlidament emès i en vigor. També es podrà consignar, abans del número del document identificador citat, el codi del país del que el subscriptor és nacional, de conformitat amb els paràmetres establerts per la norma ISO 3166 Codes (Countries), separat per un guió.
V.gr.: xinès (C) = CN; (SN) = #Pasaporte
V.gr.: xinès (C) = CN; (SN) = CN-#Pasaporte
- El número de qualsevol altre identificador assignat al posseïdor de claus pel subscriptor.
V.gr.: un número de col·legiat.
- En cas que l'"Organization" del "Subject" (això és, l'ens subscriptor) no estigui sotmès a dret espanyol, la semàntica del "SerialNumber" dependrà de la normativa aplicable conforme al "countryName" d'aquest ens.

| Camp | Descripció Contingut | Valor | Obligat |
|---------------------------------|---|--|---------------|
| 1.6.5. Country (C) | OID: 2.5.4.6 | Codi de 2 lletres del país de l'ens subscriptor. | Sí |
| 1.6.6. Organization (O) | OID: 2.5.4.10 | Nom legal de l'ens subscriptor | Sí |
| 1.6.7. Organizational Unit (OU) | OID: 2.5.4.11 | Departament/Unitat | NO |
| 1.6.8. Organizational Unit (OU) | OID: 2.5.4.11 | "Vegeu https://www.aoc.cat/CATCert/Regulacio " | Sí |
| 1.6.9. Title (T) | OID: 2.5.4.12 | Categoria i càrrec del posseïdor de claus | NO |
| 1.7. Subject Public Key Info | | | Sí |
| 1.7.1. Min Key Length | | 2048 | Sí |
| 1.7.2. Algorithm ID | | | Sí |
| 1.7.2.1. Identifier | OID: 2.5.8.1.1 | | Sí |
| 1.7.2.2. Description | | X.509 defined RSA encryption algorithm. | Sí |
| 2. X.503v3 Extensions | | | |
| 2.1. Authority Key Identifier | OID: 2.5.29.35 | | Sí |
| 2.1.1. Key Identifier | Identificador de la clau pública de l'EC emisora | | |
| 2.2. Subject Key Identifier | OID: 2.5.29.14 | | Sí |
| 2.2.1. Key Identifier | Identificador de la clau pública del posseïdor de claus | | |
| 2.3. Key Usage | Aquest camp es marca com crític | | Sí (i crític) |
| 2.3.1. Digital Signature | | True ("1") | Sí |
| 2.3.2. Non Repudiation | | True ("1") | Sí |

| Camp | Descripció Contingut | Valor | Obligat |
|------------------------------------|----------------------|---|---------|
| 2.3.3. Key Encipherment | | True ("1") | |
| 2.3.4. Data Encipherment | | False ("0") | |
| 2.3.5. Key Agreement | | True ("1") | |
| 2.3.6. Key Certificate Signature | | False ("0") | |
| 2.3.7. CRL Signature | | False ("0") | |
| 2.3.8. Encipher Only | | False ("0") | |
| 2.3.9. Decipher Only | | False ("0") | |
| 2.4. Certificate Policies | | | Sí |
| 2.4.1. Policy Identifier | | 1.3.6.1.4.1.15096.1.3.1.81.2.4 | Sí |
| 2.4.2. Policy Qualifier ID | | | Sí |
| 2.4.2.1. CPS Pointer | | https://www.aoc.cat/CATCert/Regulacio | Sí |
| 2.4.2.2. User Notice | | "Certificat personal reconegut d'identificació i signatura reconeguda, de classe 1. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A " | Sí |
| 2.5. Subject Alternative Names | | | Sí |
| 2.5.1. GeneralNames | | | |
| 2.5.1.1. rfc822Name | | <i>Correu electrònic del posseïdor de claus</i> | Sí |
| 2.5.1.2. directoryName | | | |
| 2.5.1.2.1. SerialNumber | | <i>CIF de l'ens subscriptor</i> | Sí |
| 2.5.1.3. otherName | | | |
| 2.5.1.3.1. userPrincipalName (UPN) | | <i>Usuari en el domini Windows del posseïdor de claus</i> | No |

| Camp | Descripció Contingut | Valor | Obligat |
|--------------------------------------|------------------------|---|---------|
| 2.6. Extended Key Usage | | | Sí |
| 2.6.1. emailProtection | <i>Present</i> | 1.3.6.1.5.5.7.3.4 | Sí |
| 2.6.2. TLSWebClientAuth | <i>Present</i> | 1.3.6.1.5.5.7.3.2 | Sí |
| 2.6.3. SmartCardLogon | <i>Present</i> | | |
| 2.7. cRLDistributionPoint | | | Sí |
| 2.7.1. distributionPoint | | http://epsd.catcert.net/crl/ec-sectorpublic.crl | Sí |
| 2.8. Authority Info Access | | | Sí |
| 2.8.1. AccessDescription | | | |
| 2.8.1.1. Access Method | <i>id-ad-ocsp</i> | 1.3.6.1.5.5.7.48.1 | Sí |
| 2.8.1.2. Access Location | | http://ocsp.catcert.cat | Sí |
| 2.9. AccessDescription | | | |
| 2.9.1.1. Access Method | <i>id-ad-calssuers</i> | 1.3.6.1.5.5.7.48.2 | Sí |
| 2.9.1.2. Access Location | | http://www.catcert.cat/descarrega/ec-sectorpublic.crt | Sí |
| 2.10. QualifiedCertificateStatements | | | |
| 2.10.1. QcCompliance | <i>Present</i> | | Sí |
| 2.10.2. QcRetentionPeriod | | | Sí |
| 2.10.2.1. QcEuRetentionPeriod | | 15 | |
| 2.10.3. QcSSCD | <i>Present</i> | | Sí |