

Estructura del certificat CPIXSA-2 CEX d'EC-idCAT

Control documental

| | | |
|--------------------------------|--|-------------------------------------|
| Estat formal | Elaborat per: OFICINA DE POLÍTIQUES | Aprovat per: DIRECCIÓ |
| Data de creació | 25/02/2010 | |
| Control de versions | Data: | 25/02/2010 |
| | Descripció: | Creació del document |
| Nivell accés informació | pública | |
| Títol | Estructura del certificat CPIXSA-2 CEX d'EC-idCAT | |
| Fitxer | D1112 N-Perfil CPIXSA-2 CEX EC-idCAT.pdf | |
| Control de còpies | Només les còpies disponibles a la web de CATCert 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

| | |
|---|----------|
| Control documental..... | 2 |
| Índex..... | 3 |
| 1. CPIXSA-2 CEX d'EC-idCAT | 4 |

1. CPIXSA-2 CEX d'EC-idCAT

| 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 | | Sí | |
| 1.3.1. Identifier | 1.2.840.113549.1.1.5 | | |
| 1.3.2. Description | SHA-1 with RSA Encryption | | |
| 1.4. Issuer Distinguished Name | | | |
| 1.4.1. Common Name (CN) | EC-IDCat | Sí | |
| 1.4.2. Country (C) | ES | Sí | |
| 1.4.3. Locality (L) | Passatge de la Concepció 11 08008 Barcelona | Sí | |
| 1.4.4. Organization (O) | Agència Catalana de Certificació (NIF Q-0801176-I) | Sí | |
| 1.4.5. Organizational Unit (OU) | Serveis Públics de Certificació ECV-2 | Sí | |
| 1.4.6. Organizational Unit (OU) | Vegeu https://www.catcert.net/verCIC-2 (c)03 | Sí | |
| 1.4.7. Organizational Unit (OU) | Entitat pública de certificació de ciutadans | Sí | |
| 1.5. Validity | | | |
| 1.5.1. Validity Period | 4 anys | Sí | |
| 1.6. Subject | | | |
| 1.6.1. Common Name (CN) | 2.5.4.3 Nom i cognoms del posseïdor de claus | Sí | |
| 1.6.2. Given Name (G) | 2.5.4.42 Nom del posseïdor de claus | Sí | |
| 1.6.3. Surname (SN) | 2.5.4.4 Cognoms del posseïdor de claus | Sí | |
| 1.6.4. Serial Number | 2.5.4.5 NIF/NIE del posseïdor de claus | Sí | |
| 1.6.5. Country (C) | 2.5.4.6 Codi de 2 lletres del país del posseïdor de claus | Sí | |
| 1.6.6. Organizational Unit (OU) | 2.5.4.11 Serveis Públics de Certificació CPIXSA-2 | Sí | |
| 1.6.7. Organizational Unit (OU) | 2.5.4.11 Vegeu https://www.catcert.cat/veridCAT-CEX (c) 05 | Sí | |
| 1.7. Subject Public Key Info | | | |
| 1.7.1. Min Key Length | 1024 | Sí | |
| 1.7.2. Algorithm ID | | Sí | |
| 1.7.2.1. Identifier | 2.5.8.1.1 | Sí | |
| 1.7.2.2. Description | X.509 defined RSA encryption algorithm. | Sí | |
| 2. X.509v3 Extensions | | | |
| 2.1. Authority Key Identifier | 2.5.29.35 | Sí | |
| 2.2. Subject Key Identifier | 2.5.29.14 | Sí | |
| 2.3. Key Usage | | Sí | Sí |
| 2.3.1. Digital Signature | true | | |

| Camp | Contingut | Obligat | Crític |
|-------------------------------------|---|---------|--------|
| 2.3.2. Non Repudiation | true | | |
| 2.3.3. Key Encipherment | true | | |
| 2.3.4. Data Encipherment | false | | |
| 2.3.5. Key Agreement | false | | |
| 2.3.6. Key Certificate Signature | false | | |
| 2.3.7. CRL Signature | false | | |
| 2.3.8. Encipher Only | false | | |
| 2.3.9. Decipher Only | false | | |
| 2.4. Certificate Policies | | Sí | |
| 2.4.1. Policy Information | | | |
| 2.4.1.1. Policy Identifier | | | |
| 2.4.1.1.1. Identifier | 1.3.6.1.4.1.15096.1.3.1.86.2 | | |
| 2.4.1.2. Policy Qualifiers | | | |
| 2.4.1.2.1. CPSuri | https://www.catcert.cat/veridCAT-CEX | | |
| 2.4.1.2.2. User Notice | Aquest es un certificat personal idCAT-CEX, reconegut d'identificació, signatura i xifrat de classe 2 individual. Vegeu https://www.catcert.cat/veridCAT-CEX | | |
| 2.5. Subject Alternate Name | | Sí | |
| 2.5.1. General Names | | | |
| 2.5.1.1. rfc822Name | | | |
| 2.5.1.1.1. Valor establert | Correu electrònic del posseïdor de claus | | |
| 2.5.1.2. Directory Name | | | |
| 2.5.1.2.1. Common Name (CN) | 2.5.4.3 Nom i cognoms del posseïdor de claus | | |
| 2.5.1.2.2. Serial Number | 2.5.4.5 CIF del subscriptor | | |
| 2.5.1.2.3. Country (C) | 2.5.4.6 Codi de 2 lletres del país del posseïdor de claus | | |
| 2.5.1.2.4. Organization (O) | 2.5.4.10 Agència Catalana de Certificació | | |
| 2.5.1.2.5. Organizational Unit (OU) | 2.5.4.11 IDCAT | | |
| 2.6. Issuer Alternative Name | | Sí | |
| 2.6.1. General Names | | | |
| 2.6.1.1. rfc822Name | ec_idcat@catcert.net | | |
| 2.7. Subject Directory Attributes | | Sí | |
| 2.7.1. Subject Directory Attribute | | | |
| 2.7.1.1. Valor establert | Codi de país de residència | | |
| 2.7.2. Subject Directory Attribute | | | |
| 2.7.2.1. Valor establert | Codi de país de neixament | | |
| 2.8. ExtendedKeyUsages | | Sí | |
| 2.8.1. TLSWebClientAuth | Present | | |
| 2.8.2. EmailProtection | Present | | |

| Camp | Contingut | Obligat | Crític |
|--|--|---------|--------|
| 2.9. CRL Distribution Points | | Sí | |
| 2.9.1. Distribution Point | | | |
| 2.9.1.1. Distribution Point Name | | | |
| 2.9.1.1.1. Full Name | http://epsd.catcert.net/crl/ec-idcat.crl | | |
| 2.9.2. Distribution Point | | | |
| 2.9.2.1. Distribution Point Name | | | |
| 2.9.2.1.1. Full Name | http://epsd2.catcert.net/crl/ec-idcat.crl | | |
| 2.10. Authority Information Access | | Sí | |
| 2.10.1. Access Description | | | |
| 2.10.1.1. OCSP Access Method | | | |
| 2.10.1.1.1. Access Location | http://ocsp.catcert.cat | | |
| 2.10.2. Access Description | | | |
| 2.10.2.1. calssuersAccessMethod | | | |
| 2.10.2.1.1. Access Location | http://www.catcert.cat/descarrega/ec-idcat.crt | | |
| 2.11. Netscape Certificate Type | | Sí | |
| 2.11.1. SSLClient | true | | |
| 2.11.2. SSLServer | false | | |
| 2.11.3. SMIME | true | | |
| 2.11.4. ObjectSigning | false | | |
| 2.11.5. Reserved | false | | |
| 2.11.6. SSLCA | false | | |
| 2.11.7. SMIMECA | false | | |
| 2.11.8. ObjectSigningCA | false | | |
| 2.12. Qualified Certificate Statements | | Sí | |
| 2.12.1. QcCompliance | Present | | |
| 2.12.2. QcRetentionPeriod | | | |
| 2.12.2.1. QcEuRetentionPeriod | | | |
| 2.12.2.1.1. Valor establert | 15 | | |
| 2.13. Device Identifier | | Sí | |
| 2.13.1. Supported Device | | | |
| 2.13.1.1. Device Type | Non-Cryptographic Device | | |