# Estructura del certificat
# CIC-2 SAFP d'EC-GENCAT

006_20070524

# Control documental

| | | | |
|---|---|---|---|
| **Estat formal** | **Elaborat per:**<br><br>OFICINA DE POLÍTIQUES | | **Aprovat per:**<br><br>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 CIC-2 SAFP d'EC-GENCAT | | |
| **Fitxer** | D1112 N-Perfil CIC-2 SAFP EC-GENCAT.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. | | |

006_20070524

# Índex

*Control documental* ..... 2
*Índex* ..... 3
*1. CIC-2 SAFP d'EC-GENCAT* ..... 4

006_20070524

# 1. CIC-2 SAFP d'EC-GENCAT

| 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-GENCAT | Sí | |
| 1.4.2. Country (C) | ES | Sí | |
| 1.4.3. Organization (O) | Agencia Catalana de Certificacio (NIF Q-0801176-I) | Sí | |
| 1.4.4. Organizational Unit (OU) | Serveis Publics de Certificacio ECV-1 | Sí | |
| 1.4.5. Organizational Unit (OU) | Vegeu https://www.catcert.net/verCIC-1 (c)03 | Sí | |
| 1.4.6. Organizational Unit (OU) | Generalitat de Catalunya | Sí | |
| 1.5. Validity | | | |
| 1.5.1. Validity Period | 16 anys | Sí | |
| 1.6. Subject | | | |
| 1.6.1. Common Name (CN) | 2.5.4.3<br>EC-SAFP | Sí | |
| 1.6.2. Country (C) | 2.5.4.6<br>ES | Sí | |
| 1.6.3. Locality (L) | 2.5.4.7<br>Passatge de la Concepcio 11 08008 Barcelona | Sí | |
| 1.6.4. Organization (O) | 2.5.4.10<br>Agencia Catalana de Certificacio (NIF Q-0801176-I) | Sí | |
| 1.6.5. Organizational Unit (OU) | 2.5.4.11<br>Serveis Publics de Certificacio ECV-2 | Sí | |
| 1.6.6. Organizational Unit (OU) | 2.5.4.11<br>Vegeu https://www.catcert.net/verCIC-2 (c)03 | Sí | |
| 1.6.7. Organizational Unit (OU) | 2.5.4.11<br>Secretaria d'Administracio i Funcio Publica | Sí | |
| 1.7. Subject Public Key Info | | | |
| 1.7.1. Min Key Length | 2048 | 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 | false | | |
| 2.3.2. Non Repudiation | false | | |

006_20070524

| Camp | Contingut | Obligat | Crític |
|---|---|---|---|
| 2.3.3. Key Encipherment | false | | |
| 2.3.4. Data Encipherment | false | | |
| 2.3.5. Key Agreement | false | | |
| 2.3.6. Key Certificate Signature | true | | |
| 2.3.7. CRL Signature | true | | |
| 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 | 1.3.6.1.4.1.15096.1.3.1.12 | | |
| 2.4.1.2. Policy Qualifiers | | | |
| 2.4.1.2.1. CPSuri | https://www.catcert.net/verCIC-2 | | |
| 2.4.1.2.2. User Notice | Aquest certificat és emès única i exclusivament a Entitats de Certificació de nivell 2. Vegeu https://www.catcert.net/verCIC-2 | | |
| 2.5. Basic Constraints | | Sí | Sí |
| 2.5.1. CA | true | | |
| 2.5.2. Path Len Constraint | Cap | | |
| 2.6. Subject Alternate Name | | Sí | |
| 2.6.1. General Names | | | |
| 2.6.1.1. rfc822Name | ec_safp@catcert.net | | |
| 2.7. Issuer Alternative Name | | Sí | |
| 2.7.1. General Names | | | |
| 2.7.1.1. rfc822Name | ec_gencat@catcert.net | | |
| 2.8. CRL Distribution Points | | Sí | |
| 2.8.1. Distribution Point | | | |
| 2.8.1.1. Distribution Point Name | | | |
| 2.8.1.1.1. Full Name | http://epscd.catcert.net/crl/ec-gencat.crl | | |
| 2.8.1.1.2. Full Name | http://epscd2.catcert.net/crl/ec-gencat.crl | | |

006_20070524