Agència Catalana de Certificació

# Estructura dels certificats CDA-1 Segell electrònic (nivells alt i mig)

| | |
|---|---|
| Referència: | D1112 N-Perfil CDA-1 Segell electrònic |
| Versió: | 1.10 |
| Data: | 26/11/2008 |

Agència Catalana de Certificació

# Informació general

## Control documental

| | |
|---|---|
| **Projecte:** | Agència Catalana de Certificació |
| **Entitat de destinació:** | |
| **Títol:** | Estructura dels certificats CDA-1 Segell electrònic (nivells mig i alt). |
| **Codi de referència:** | |
| **Versió:** | 1.10 |
| **Data:** | 26/11/2008 |
| **Fitxer:** | D1112 N-Perfil CDA-1 Segell electrònic v1r9.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<br>Data: 02/03/2008 | Nom: Àrea d'AiR<br>Data: 26/11/2008 | Nom:<br>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 | 09/04/2008 | Henao | | Document independent per als CDA-1 Segell electrònic |
| 1.7 | 22/04/2008 | Cruellas | | Esmena QcEuRetentionPeriod |
| 1.8 | 08/05/2008 | Cruellas | | Esmena numeració CDA-1 Segell electrònic Nivell Mig |
| 1.9 | 22/05/2008 | Cruellas | | Revisió conforme a modificacions en els perfils de referència del MAP |
| 1.10 | 26/11/2008 | Cruellas | | Unificació de la descripció dels camps `1.6.6. Common Name (CN)` i `2.6.2.5. Denominació del sistema o component` |

# Índex

# 1. CDA-1 Segell electrònic de nivell alt

Certificat de dispositiu d'aplicació digitalment assegurada, de Segell Electrònic, 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 CDA.

| 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 | Segons cada EC | Sí | |
| 1.5. Validity | 3 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) | "ES" | 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 CDA-1 Segell electrònic" | Sí | |
| 1.6.5. Organizational Unit (OU) | "Vegeu https://www.catcert.net/verCDA-1 Segell (c)08" | Sí | |
| 1.6.6. Common Name (CN) | Denominació del sistema, aplicació o component d'actuació automatitzada que posseeix el certificat de segell | Sí | |
| 1.6.7. Serial Number | NIF del subscriptor | Sí | |
| 1.6.8. Surname | Cognoms del responsable | No | |
| 1.6.9. Given Name | Nom del responsable | 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 | | | |

| Camp | Contingut | Obligat | Crític |
|---|---|---|---|
| 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 | Seleccionat “1” | Sí | |
| 2.3.3. Key Encipherment | Seleccionat “1” | Sí | |
| 2.3.4. Data Encipherment | Seleccionat “1” | Sí | |
| 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. 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 | |
| 2.4.3. QcSSCD | OID 0.4.0.1862.1.4 | Sí | |
| 2.5. Certificate Policies | | Sí | |
| 2.5.1. Policy Identifier | CATCert.1.3.1.91.2 | Sí | |
| 2.5.2. Policy Qualifier ID | | Sí | |
| 2.5.2.1. CPS Pointer | https://www.catcert.net/verCDA-1 Segell | Sí | |
| 2.5.2.2. User Notice | “Aquest és un certificat reconegut de segell electrònic amb conformitat amb la llei 11/2007, de classe 1 i nivell alt. Vegeu https://www.catcert.net/verCDA-1 Segell “ | Sí | |
| 2.6. Subject Alternate Names | | Sí | |
| 2.6.1. rfc822Name | Correu electrònic del servei | Sí | |
| 2.6.2. Directory Name | Identitat Administrativa | Sí | |
| 2.6.2.1. Tipus de certificat | “Certificat de segell electrònic, de classe 1, nivell alt” OID: 1.3.6.1.4.1.14862.1.4.3.1.1 | Sí | |
| 2.6.2.2. Nom de l’entitat subscriptora | L’entitat propietària del certificat OID: 1.3.6.1.4.1.14862.1.4.3.1.2 | Sí | |

| Camp | Contingut | Obligat | Crític |
|---|---|---|---|
| 2.6.2.3. NIF de l'entitat subscriptora | NIF de l'entitat subscriptora<br>OID: 1.3.6.1.4.1.14862.1.4.3.1.3 | Sí | |
| 2.6.2.4. DNI/NIE del responsable | DNI/NIE del responsable del segell<br>OID: 1.3.6.1.4.1.14862.1.4.3.1.4 | NO | |
| 2.6.2.5. Denominació del sistema o component | Denominació del sistema, aplicació o component d'actuació automatitzada que posseeix el certificat de segell [1]<br>OID: 1.3.6.1.4.1.14862.1.4.3.1.5 | Sí | |
| 2.6.2.6. Nom de pila | Nom de pila del responsable del certificat<br>OID: 1.3.6.1.4.1.14862.1.4.3.1.6 | NO | |
| 2.6.2.7. Primer cognom | Primer cognom del responsable del certificat<br>OID: 1.3.6.1.4.1.14862.1.4.3.1.7 | NO | |
| 2.6.2.8. Segon cognom | Segon cognom del responsable del certificat<br>OID: 1.3.6.1.4.1.14862.1.4.3.1.8 | NO | |
| 2.6.2.9. Correu electrònic | Correu electrònic del responsable del segell<br>OID: 1.3.6.1.4.1.14862.1.4.3.1.9 | NO | |
| 2.7. Issuer Alternative Name | | Sí | |
| 2.7.1. rfc822Name | ec_xxx@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://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 Access Location | http://ocsp.catcert.net | Sí | |

[1] El contingut d'aquest camp ha de coincidir amb l'especificat al "CommonName" del "Subject" (1.6.6.).

# 2. CDA-1 Segell electrònic de nivell mig

Certificat de dispositiu d'aplicació digitalment assegurada, de Segell Electrònic, 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 CDA.

| 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 | Segons cada EC | Sí | |
| 1.5. Validity | 3 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) | ES | 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 CDA-1 Segell electrònic" | Sí | |
| 1.6.5. Organizational Unit (OU) | "Vegeu https://www.catcert.net/verCDA-1 Segell (c)08" | Sí | |
| 1.6.6. Common Name (CN) | Denominació del sistema, aplicació o component d'actuació automatitzada que posseeix el certificat de segell | Sí | |
| 1.6.7. Serial Number | NIF del subscriptor | Sí | |
| 1.6.8. Surname | Cognoms del responsable | No | |
| 1.6.9. Given Name | Nom del responsable | No | |
| 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 | | | |

| Camp | Contingut | Obligat | Crític |
|---|---|---|---|
| 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 | Seleccionat “1” | Sí | |
| 2.3.3. Key Encipherment | Seleccionat “1” | Sí | |
| 2.3.4. Data Encipherment | Seleccionat “1” | Sí | |
| 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. 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 | |
| 2.5. Certificate Policies | | Sí | |
| 2.5.1. Policy Identifier | CATCert.1.3.1.91.1 | Sí | |
| 2.5.2. Policy Qualifier ID | | Sí | |
| 2.5.2.1. CPS Pointer | https://www.catcert.net/verCDA-1Segell | Sí | |
| 2.5.2.2. User Notice | “Aquest és un certificat de segell electrònic amb conformitat amb la llei 11/2007, de classe 1 i nivell mig. Vegeu https://www.catcert.net/verCDA-1Segell” | Sí | |
| 2.6. Subject Alternate Names | | Sí | |
| 2.6.1. rfc822Name | Correu electrònic del servei | Sí | |
| 2.6.2. Directory Name | Identitat administrativa | Sí | |
| 2.6.2.1. Tipus de certificat | “Certificat de segell electrònic, de classe 1, nivell mig” OID: 1.3.6.1.4.1.14862.1.4.3.2.1 | Sí | |
| 2.6.2.2. Nom de l’entitat subscriptora | L’entitat propietària del certificat OID: 1.3.6.1.4.1.14862.1.4.3.2.2 | Sí | |
| 2.6.2.3. NIF de l’entitat subscriptora | NIF de l’entitat subscriptora OID: 1.3.6.1.4.1.14862.1.4.3.2.3 | Sí | |

| Camp | Contingut | Obligat | Crític |
|---|---|---|---|
| 2.6.2.4. DNI/NIE del responsable | DNI/NIE del responsable del segell<br>OID: 1.3.6.1.4.1.14862.1.4.3.2.4 | NO | |
| 2.6.2.5. Denominació del sistema o component | Denominació del sistema, aplicació o component d'actuació automatitzada que posseeix el certificat de segell [2]<br>OID: 1.3.6.1.4.1.14862.1.4.3.2.5 | Sí | |
| 2.6.2.6. Nom de pila | Nom de pila del responsable del certificat<br>OID: 1.3.6.1.4.1.14862.1.4.3.2.6 | NO | |
| 2.6.2.7. Primer cognom | Primer cognom del responsable del certificat<br>OID: 1.3.6.1.4.1.14862.1.4.3.2.7 | NO | |
| 2.6.2.8. Segon cognom | Segon cognom del responsable del certificat<br>OID: 1.3.6.1.4.1.14862.1.4.3.2.8 | NO | |
| 2.6.2.9. Correu electrònic | Correu electrònic del responsable del segell<br>OID: 1.3.6.1.4.1.14862.1.4.3.2.9 | NO | |
| 2.7. Issuer Alternative Name | | Sí | |
| 2.7.1. rfc822Name | ec_xxx@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://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. Access Location | http://ocsp.catcert.net | Sí | |

[2] El contingut d'aquest camp ha de coincidir amb l'especificat al "CommonName" del "Subject" (1.6.6.).