

# Estructura del certificat CDA-1 SENM d'EC-AL

## Control documental

<b>Estat formal</b>	<b>Elaborat per:</b>  OFICINA DE POLÍTIQUES	<b>Aprovat per:</b>  DIRECCIÓ
<b>Data de creació</b>	23/02/2010	
<b>Control de versions</b>	<b>Data:</b>	23/02/2010
	<b>Descripció:</b>	Creació del document
<b>Nivell accés informació</b>	pública	
<b>Títol</b>	Estructura del certificat CDA-1 SENM d'EC-AL	
<b>Fitxer</b>	D1112 N-Perfil CDA-1 SENM EC-AL.pdf	
<b>Control de còpies</b>	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.	
<b>Drets d'autor</b>	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 <a href="http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca">http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca</a> o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.	

## Índex

---

<b>Control documental.....</b>	<b>2</b>
<b>Índex.....</b>	<b>3</b>
<b>1. CDA-1 SENM d'EC-AL .....</b>	<b>4</b>

## 1. CDA-1 SENM d'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		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-AL	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 <a href="https://www.catcert.net/verCIC-2">https://www.catcert.net/verCIC-2</a> (c)03	Sí	
1.4.7. Organizational Unit (OU)	Administracions Locals de Catalunya	Sí	
1.5. Validity			
1.5.1. Validity Period	3 anys	Sí	
1.6. Subject			
1.6.1. Common Name (CN)	2.5.4.3 Denominació del sistema, aplicació o component d'actuació automatitzada que posseeix el certificat de segell	Sí	
1.6.2. Given Name (G)	2.5.4.42 Nom del responsable	Sí	
1.6.3. Surname (SN)	2.5.4.4 Cognoms del responsable	Sí	
1.6.4. Serial Number	2.5.4.5 NIF del subscriptor	Sí	
1.6.5. Country (C)	2.5.4.6 Codi de 2 lletres del país del posseïdor de claus	Sí	
1.6.6. Organization (O)	2.5.4.10 Nom legal del subscriptor - Entitat de Registre	Sí	
1.6.7. Organizational Unit (OU)	2.5.4.11 Departament/Unitat	No	
1.6.8. Organizational Unit (OU)	2.5.4.11 Serveis Públics de Certificació CDA-1 Segell de nivell mig	Sí	
1.6.9. Organizational Unit (OU)	2.5.4.11 Vegeu <a href="https://www.catcert.cat/verCDA-1Segell">https://www.catcert.cat/verCDA-1Segell</a> (c)08	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	

Camp	Contingut	Obligat	Crític
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		
2.3.2. Non Repudiation	true		
2.3.3. Key Encipherment	true		
2.3.4. Data Encipherment	true		
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	1.3.6.1.4.1.15096.1.3.1.91.1		
2.4.1.2. Policy Qualifiers			
2.4.1.2.1. CPSuri	<a href="https://www.catcert.cat/verCDA-1Segell">https://www.catcert.cat/verCDA-1Segell</a>		
2.4.1.2.2. User Notice	Aquest és un certificat de segell electrònic amb conformitat amb la llei 11/2007, de classe 1 i nivell mig. Vegeu <a href="https://www.catcert.cat/verCDA-1Segell">https://www.catcert.cat/verCDA-1Segell</a>		
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 servei		
2.5.1.2. Directory Name			
2.5.1.2.1. Atribut privat	1.3.6.1.4.1.14862.1.4.3.2.1 Certificat de segell electrònic, de classe 1, nivell mig		
2.5.1.2.2. Atribut privat	1.3.6.1.4.1.14862.1.4.3.2.2 Nom de l'entitat propietària del certificat		
2.5.1.2.3. Atribut privat	1.3.6.1.4.1.14862.1.4.3.2.3 CIF de l'entitat subscriptora		
2.5.1.2.4. Atribut privat	1.3.6.1.4.1.14862.1.4.3.2.4 DNI/NIE del responsable del segell		
2.5.1.2.5. Atribut privat	1.3.6.1.4.1.14862.1.4.3.2.5 Denominació del sistema, aplicació o component d'actuació automatitzada que posseeix el certificat de segell		
2.5.1.2.6. Atribut privat	1.3.6.1.4.1.14862.1.4.3.2.6 Nom de pila del responsable del certificat		
2.5.1.2.7. Atribut privat	1.3.6.1.4.1.14862.1.4.3.2.7 Primer cognom del responsable del certificat		
2.5.1.2.8. Atribut privat	1.3.6.1.4.1.14862.1.4.3.2.8 Segon cognom del responsable del certificat		
2.5.1.2.9. Atribut privat	1.3.6.1.4.1.14862.1.4.3.2.9 Correu electrònic del responsable del segell		

Camp	Contingut	Obligat	Crític
2.6. ExtendedKeyUsages		Sí	
2.6.1. TLSWebClientAuth	Present		
2.6.2. EmailProtection	Present		
2.7. CRL Distribution Points		Sí	
2.7.1. Distribution Point			
2.7.1.1. Distribution Point Name			
2.7.1.1.1. Full Name	http://epsd.catcert.net/crl/ec-al.crl		
2.7.1.1.2. Full Name	http://epsd2.catcert.net/crl/ec-al.crl		
2.8. Authority Information Access		Sí	
2.8.1. Access Description			
2.8.1.1. OCSP Access Method			
2.8.1.1.1. Access Location	http://ocsp.catcert.cat		
2.8.2. Access Description			
2.8.2.1. caIssuersAccessMethod			
2.8.2.1.1. Access Location	http://www.catcert.cat/descarrega/al_csrs.crt		
2.9. Netscape Certificate Type		Sí	
2.9.1. SSLClient	true		
2.9.2. SSLServer	false		
2.9.3. SMIME	true		
2.9.4. ObjectSigning	false		
2.9.5. Reserved	false		
2.9.6. SSLCA	false		
2.9.7. SMIMECA	false		
2.9.8. ObjectSigningCA	false		
2.10. Qualified Certificate Statements		Sí	
2.10.1. QcCompliance	Present		
2.10.2. QcRetentionPeriod			
2.10.2.1. QcEuRetentionPeriod			
2.10.2.1.1. Valor establert	15		