



Consorci  
Administració Oberta  
de Catalunya

---

## Descripció del Perfil de certificats CDP-1

---

 Generalitat  
de Catalunya

LOCALRET

## Control documental

<b>Estat formal</b>	<b>Elaborat per:</b> Chema López	<b>Aprovat per:</b> Francesc Ferrer
<b>Data de creació</b>	23/02/2010	
<b>Control de versions</b>	<b>Versió:</b>	2.3
	<b>Data:</b>	20/01/16
	<b>Descripció:</b>	Adaptació del perfil CDP-1 per a l'EC-SectorPublic
<b>Nivell accés informació</b>	Pública	
<b>Títol</b>	Descripció del Perfil de certificats CDP-1	
<b>Fitxer</b>	D1112 N-Perfil EC-SectorPublic CDP-1 v2r3.docx	
<b>Control de còpies</b>	Només les còpies disponibles a la web del Consorci AOC a <a href="https://www.aoc.cat/CATCert/Regulacio">https://www.aoc.cat/CATCert/Regulacio</a> 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

1	Descripció del perfil CDP-1 de l'EC-SectorPublic .....	4
---	--	---

## Descripció del perfil CDP-1 de l'EC-SectorPublic

Camp	Descripció Contingut	Valor	Obliga t
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		1.2.840.113549.1.1.11	
1.3.2. Description		"SHA-256 with RSA Signature"	
1.4. Issuer Distinguished Name	<i>Establert automàticament per l'EC</i>		Sí
1.4.1. Common Name (CN)		"EC-SectorPublic"	
1.4.2. Country (C)		"ES"	
1.4.3. Organization (O)		"CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA"	
1.4.4. Organizational Unit (OU)		"Serveis Públics de Certificació"	
1.5. Validity		4 anys	Sí
1.5.1. Not Before	<i>e.g., "00:00:01 01 September 1999"</i>		
1.5.2. Not After	<i>e.g., "23:59:59 31 August 2003"</i>		

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>Nom de l'ens subscriptor – Entitat de registre – Presentació preferida pel subscriptor</i>	Sí
1.6.2. Country (C)	<i>OID: 2.5.4.6</i>	<i>Codi de 2 lletres del país de l'ens subscriptor</i>	Sí
1.6.3. Organization (O)	<i>OID: 2.5.4.10</i>	<i>Nom legal de l'ens subscriptor</i>	Sí
1.6.4. Organizational Unit (OU)	<i>OID: 2.5.4.11</i>	<i>Departament/Unitat</i>	NO
1.6.5. Organizational Unit (OU)	<i>OID: 2.5.4.11</i>	<i>"Vegeu <a href="https://www.aoc.cat/CATCert/Regulacio">https://www.aoc.cat/CATCert/Regulacio</a>"</i>	Sí
1.7. Subject Public Key Info			Sí
1.7.1. Min Key Length		2048	
1.7.2. Algorithm ID			
1. Identifier	<i>OID: 2.5.8.1.1</i>		
2. Description		X.509 defined RSA encryption algorithm.	
2. X.503v3 Extensions			
2.1. Authority Key Identifier	<i>OID: 2.5.29.35</i>		Sí
2.1.1. Key Identifier	<i>Identificador de la clau pública de l'EC emisora</i>		
2.2. Subject Key Identifier	<i>OID: 2.5.29.14</i>		Sí
2.2.1. Key Identifier	<i>Identificador de la clau pública del posseïdor de claus</i>		
2.3. Key Usage	<i>Aquest camp es marca com</i>		Sí (i)

Camp	Descripció Contingut	Valor	Obligat
	<i>crític</i>		<i>crític</i> )
2.3.1. Digital Signature		True ("1")	
2.3.2. Non Repudiation/ Content Commitment		True ("1")	
2.3.3. Key Encipherment		False ("0")	
2.3.4. Data Encipherment		False ("0")	
2.3.5. Key Agreement		False ("0")	
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		1.3.6.1.4.1.15096.1.3.1.71	
2.4.2. Policy Qualifier ID			
2.4.2.1. CPS Pointer		<a href="https://www.aoc.cat/CATCert/Regulacio">https://www.aoc.cat/CATCert/Regulacio</a>	
2.4.2.2. User Notice		»Certificat de dispositiu de signatura de programari de classe 1. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A»	
2.5. Subject Alternative Names			Sí
2.5.1. GeneralNames			
2.5.1.1. rfc822Name		<i>Correu electrònic del webmestre</i>	Sí
2.5.1.2. directoryName			
2.5.1.2.1. SerialNumber	<i>OID: 2.5.4.5</i>	<i>CIF de l'ens subscriptor</i>	Sí

Camp	Descripció Contingut	Valor	Obligat
2.6. Extended Key Usage			Sí
2.6.1. CodeSigning	<i>Present</i>	<i>id-kp-codeSigning</i> 1.3.6.1.5.5.7.3.3	
2.6.2. PrivateExtendedKeyUsage		<i>szOID_KP_LIFETIME_SIGNING</i> 1.3.6.1.4.1.311.10.3.13	
2.7. cRLDistributionPoint			Sí
2.7.1. distributionPoint		<a href="http://epsd.catcert.net/cr/ec-sectorpublic.crl">http://epsd.catcert.net/cr/ec-sectorpublic.crl</a>	
2.7.2.			
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	
2.8.1.2. Access Location		<a href="http://ocsp.catcert.cat">http://ocsp.catcert.cat</a>	
2.9. AccessDescription			
2.9.1.1. Access Method	<i>id-ad-calssuers</i>	1.3.6.1.5.5.7.48.2	
2.9.1.2. Access Location		<a href="http://www.catcert.cat/descarrega/ec-sectorpublic.crt">http://www.catcert.cat/descarrega/ec-sectorpublic.crt</a>	