Consorci
Administració Oberta
de Catalunya

Descripción del Perfil de certificados CPISA-2

Generalitat
de Catalunya

LOCALRET

Control documental

Estado formal	**Elaborado por:** **Servicio de Certificación Digital**	**Aprobado por:** **Dirección del Consorci AOC**
Fecha de creación	11/05/2018	
Control de versiones	**Versión:**	2.1
	Fecha:	11/05/2018
	Descripción:	Adaptación a eIDAS
Nivel acceso información	Pública	
Título	Descripción del Perfil de idCAT certificado – CPISA-2	
Control de copias	Únicamente las copias disponibles en la web del Consorci AOC en https://www.aoc.cat/CATCert/Regulacio grantizan la actualización de los documentos. Todas las copias impresas o depositadas en ubicaciones diferentes se considerarán copias no controladas.	
Derechos de autor	Esta obra está sujeta a una licencia Reconocimiento-No comercial-Sin obras derivadas 3.0 España de Creative Commons. Para ver una copia, visitar https://creativecommons.org/licenses/by-nc-nd/3.0/es/deed.ca o enviar una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.	

Índice

PERFIL DE LOS CERTIFICADOS **3**
Certificado 4
Extensiones de los certificados 4

PERFIL DE LOS CERTIFICADOS

Certificado

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Apellidos y Nombre del firmante+ " - DNI " + número del documento de identificación. Ex: PEREZ MAS JOSE – DNI 123456789Z
serialNumber	Número de serie	Número del documento de identidad del firmante, con la semántica propuesta por la norma ETSI EN 319 412-1[1]
SN, surName	Apellidos	Apellidos del firmante tal y como aparecen en el documento de identidad utilizado
GN, givenName	Nombre de pila	Nombre de pila del firmante, tal y como aparecen en el documento de identidad utilizada
C, Country	País	"ES"

Extensiones de los certificados

Extensión	Crítica	Valor
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Non Repudiation Key Encipherment
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenida a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.15096.1.3.2.86.2 <URI de la DPC> User Notice: "idCAT Certificat. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"

[1] SerialNumber = p. ej: IDCES-00000000G. 3 caracteres para indicar el tipo de documento (IDC= documento nacional de identidad, PAS=pasaporte, ...) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

		<OID de la política de certificación ETSI: 0.4.0.194112.1.0> (Correspondiente a la política para certificados EU cualificados emitidos a personas físicas “QCP-n”, sin uso de un DSCF)
qcStatements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificat de l’EC emisora>