Consorci
Administració Oberta
de Catalunya

Descripció del Perfil de certificats CPISA-2

Generalitat
de Catalunya

LOCALRET

Control documental

Estat formal	Elaborat per: Servei de Certificació Digital	Aprovat per: Direcció del Consorci AOC
Data de creació	11/05/2018	
Control de versions	**Versió:**	2.1
	Data:	11/05/2018
	Descripció:	Adaptació a eIDAS
Nivell accés informació	Pública	
Títol	Descripció del Perfil d'idCAT certificat – CPISA-2	
Control de còpies	Només les còpies disponibles a la web del Consorci AOC a https://www.aoc.cat/CATCert/Regulacio 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 3.0 Espanya de Creative Commons. Per veure'n una còpia, visiteu https://creativecommons.org/licenses/by-nc-nd/3.0/es/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.	

Índex

PERFIL DELS CERTIFICATS

Certificat

Camp del DN	Nom	Descripció
CN, Common Name	Nom	Cognoms i Nom del signant + " - DNI " + número del document d'identificació. Ex: PEREZ MAS JOSE – DNI 123456789Z
serialNumber	Número de serie	Número del document d'identitat del signant, amb la semàntica proposada per la norma ETSI EN 319 412-1[1]
SN, surName	Cognoms	Cognoms del signant tal i com apareixen al document d'identitat fet servir
GN, givenName	Nom de pila	Nom de pila del signant, tal i com apareixen en el document d'identitat fet servir
C, Country	País	"ES"

Extensions dels certificats

Extensió	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 clau pública del certificat, obtinguda a partir del hash de la mateixa>
X509v3 Authority Key Identifier	-	<id de la clau pública del certificat de la CA, obtingut a partir del hash de la mateixa>
X509v3 CRL Distribution Points	-	http://epscd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Certificate Policies	-	<OID de la política de certificació corresponent al certificat> 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 caràcters per indicar el tipus de document (IDC= document nacional d'identitat, PAS=passaport, ...) + 2 caràcters per identificar el país (ES) + Número d'identitat (Printable String)) Size [RFC 5280] 64

		<OID de la política de certificació ETSI: 0.4.0.194112.1.0> (Corresponent a la política per a certificats EU qualificats emesos a persones físiques “QCP-n”, sense ús d’un DSCF)
qcStatements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys 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>