CATÀLEG DE CERTIFICATS

T-CAT: Certificats electrònics qualificats d'Empleat Públic

- **T-CAT amb càrrec (CPI-1 + CPSQ-1)**

El certificat personal en targeta va adreçat a persones físiques i disposa d'informació referent al titular que permet identificar-lo i la seva organització subscriptora. Se subministra al personal de les administracions públiques catalanes com a element identificatiu en les comunicacions electròniques, permetent signar documents en format electrònic per tal de fer possible els tràmits i les consultes en línia, amb tota garantia, i agilitzant-ne les gestions. Aquest certificat permet identificar-se com a persona posseïdora d'un determinat càrrec en la seva organització

- **T-CAT P (CPISA-1)**

El certificat personal d'identificació i signatura avançada amb càrrec, opcional, és un certificat reconegut que identifica, a més de la persona que el posseeix, a la seva organització subscriptora, i pot incloure una manifestació relativa al càrrec del posseïdor de claus, està destinat als treballadors públics del sector públic català.

És una eina d'autenticació i que genera signatura avançada, donat que es lliura en programari, sense dispositiu segur de creació de signatura; de manera que es pot instal·lar en diferents suports: ordinadors, telèfons mòbils, tabletes, etc.

- **T-CAT de Representant (CPRISQ-1)**

És el certificat electrònic de representant davant les Administracions Públiques de nivell alt, que s'incorpora al Catàleg de certificats que emet el Consorci AOC amb l'adaptació a la normativa EIDAS. Aquest certificats sempre ha d'anar acompanyat d'una acreditació del nomenament com a representant. El document ha de ser una publicació al diari o butlletí oficial, inscripció en un registre públic, un document notarial, etc.. en el marc de la Llei 59/2003, de 19 de desembre, de signatura electrònica, on s'estipula al llarg del seu articulat que l'acreditació de la representació s'ha d'efectuar per mitjà de document públic.

És una eina d'identificació i signatura qualificada, que permet al representant actuar en nom de l'organisme .

- **T-CAT de Pseudònim (CPPI-1 + CPPSQ-1)**

Es tracta d'un certificat de signatura per al treballador públic amb pseudònim de nivell alt. Les dades personals no apareixeran en el certificat, ja que aquestes seran substituïdes pel pseudònim indicat. L'emissió d'aquests certificats es farà sota la valoració prèvia de l'acreditació legal del pseudònim, que haurà d'acompanyar la sol·licitud. S'acceptaran molt específicament per usos justificats en que no es puguin mostrar les dades del titular i per persones, que dins de la seva organització ja disposin de pseudònim regulat.

Els col·lectius que poden disposar d'un certificat de pseudònim són aquells que realitzin actuacions sobre: informació classificada, seguretat pública, defensa nacional o altres actuacions en les que estigui legalment justificat l'anonimat per a la realització d'actuacions.

El pseudònim sempre el proporcionarà l'Administració. Només poden sol·licitar que es desvetlli la identitat de la persona amb pseudònim: els òrgans judicials i d'altres òrgans o persones legitimades i només en els casos de l'art. 11.2 de la LOPD. En aquests casos, el Prestador de Serveis de Certificació estarà obligat a revelar la identitat del signatari.

El Règim jurídic de la informació classificada està regular per la Llei 9/1968, de 5 d'abril, sobre secrets oficials i el Decret 242/1969, de 20 de febrer, que la desenvolupa.

El pseudònim pot ser un número d'identificació professional (NIP) sempre que no estigui relacionat amb dades personals com el DNI i alternativament altres indicadors.

- **T-CAT d'operador d'entitat de registre T-CAT (CIPISR-1)**

Aquest certificat va adreçat a persones físiques que han de desenvolupar responsabilitats d'operador a una entitat de registre T-CAT. Aquestes entitats, que col·laboren amb el Consorci AOC en l'emissió de certificats, requereixen de certificats digitals per tal d'operar amb les aplicacions de generació i gestió de certificats.

Al contrari que la resta de certificats T-CAT personals, no permet el xifrat de documents ni la realització de tràmits davant de les administracions públiques. Això és degut a que la seva funció és únicament la d'identificar els operadors que accedeixen a les aplicacions de l'ER T-CAT i permetre la signatura de les operacions realitzades.

T-CAT: Certificats electrònics qualificats de segell electrònic de l'administració pública

- **Certificat de Segell electrònic (CDA-1 SGNM)**

És un certificat digital que serveix per a la identificació i l'autenticació de l'exercici de la competència en l'actuació administrativa automatitzada, segons l'article 42 de la Llei 40/2015 de regim jurídic de sector públic.

Aquest certificat pot utilitzar-se per a l'intercanvi de dades (entre administracions, administracions i ciutadans i entre administracions i empreses), la identificació i autenticació d'un sistema, servei web o aplicació, l'arxiu electrònic automatitzat, les compulses i còpies electròniques, entre d'altres.

Aquest certificat és recomanable per a la majoria de les administracions públiques que poden tenir els següents riscos: infracció de seguretat (p.e. robatori de la identitat), pèrdues econòmiques moderades, pèrdua d'informació sensible o crítica o refutació d'una transacció amb impacte econòmic significatiu.

T-CAT: Certificats aplicació

- **Certificat d'aplicació (CDA-1)**

Aquest certificat s'emmagatzema en un servidor (preferiblement en un dispositiu criptogràfic) i és requerit per una aplicació per signar documents o missatges per assegurar l'autenticitat i integritat dels missatges o fitxers signats.

El seu ús equival a un tampó de l'ens o departament.

No és un certificat personal, sinó que està vinculat a una aplicació i actua de manera síncrona, pel que no requereix la intervenció de cap operador.

Cal dimensionar bé el maquinari on residirà aquest certificat, ja que les tasques de signatura asimètrica poden saturar-lo. Tanmateix, l'accés al maquinari ha d'estar restringit i protegit per evitar possibles usos fraudulents del certificat.

T-CAT: Certificats de dispositiu

Certificats de component SSL

- **Certificat dispositiu servidor segur (CDS-1)**

Quan es parla de servidors segurs, ens referim a servidors web que fan servir un protocol de comunicacions que els protegeix i els fa més segurs. És molt comú que els servidors web facin servir el protocol SSL (*Secure Sockets Layer*) o TSL *(Transport Layer Security)*, que ofereix els següents serveis de seguretat:

- Identifica al servidor web davant l'usuari.
- Xifra les dades intercanviades entre l'usuari i el servidor.
- Permet la identificació dels clients a partir dels seus certificats T-CAT personals.

Els certificats de dispositiu servidor (CDS) s'han d'instal·lar als servidors web de les administracions públiques catalanes en dominis que es trobin registrats públicament . Així s'assegura la seva identitat del domini davant dels usuaris que s'hi connecten.

Garanteix, a més, que el lloc web és l'original, el domini està oficialment registrat, és vàlid, no ha estat suplantat, i que ningú ha pogut alterar la informació publicada ni manipular les dades enregistrades en el servidor de manera no autoritzada. Per tant, podem dir que un certificat de servidor segur determina que un lloc web és genuí.

Per altra banda, si cal un servidor web que funcioni amb protocol SSL, pot configurar-se per demanar al client que intenta connectar-se que s'identifiqui mitjançant el seu certificat digital. D'aquesta manera, és possible implementar fàcilment un mecanisme de control d'accés a una zona web.

Certificats de electrònic d'autenticació de llocs web

- **Certificat dispositiu de servidor segur *extended validation* (CDSQ-1)**

Els certificats de dispositiu de servidor segur EV no són estructuralment o funcionalment diferents dels CDS ordinaris, però es diferencien d'aquests en què han estat emesos per entitats de certificació que, com el Consorci AOC, han superat els estrictes requisits de seguretat que estableix *l'Standard Extended Validation SSL Certificate* i que, per tant, garanteixen el màxim nivell de seguretat en les transaccions dels llocs web que en facin ús.

El principal avantatge és, un cop es materialitzi tècnicament el reconeixement *Extended validation* amb Microsoft i Firefox, que els nous navegadors web els acceptaran immediatament i mostraran una confirmació de seguretat (imatge inferior) que permetrà als usuaris identificar ràpidament un lloc segur i de confiança, ja que estan dissenyats per a mostrar senyals visuals úniques que indiquen la presència d'un certificat EV.

Els certificats de dispositiu de servidor segur EV es necessari que el domini estigui registrat públicament a nom de l'ens sol·licitant i que sigui vigent.

Certificats qualificats de seu electrònica de l'administració Pública

- **Certificat de Seu electrònica de nivell mig (CDS-1 SENM)**

Aquest és un certificat digital de dispositiu que serveix per identificar i garantir una comunicació segura amb la seu electrònica d'un ens, entenent seu electrònica en els termes que descriu la Llei 40/2015 de règim jurídic del sector públic en el seu article 38 (40/2015)

Aquest certificat pot utilitzar-se per a la connexió segura dels ciutadans a pàgines web oficials, l'autenticació d'un lloc web, l'allotjament de registres electrònics, la consulta i autorització de registres de representació, etc.

Des de 2011, el Consorci AOC emet el certificat de Seu tot seguint *l'Standard Extended Validation SSL Certificate*, fet que garanteix el màxim nivell de seguretat en les transaccions que es realitzin en el lloc web que en faci ús.

Els requisits per obtenir els certificats de dispositiu els trobareu al Manual Sol·licitud SSL.

QUADRE RESUM

	Producte	Acrònims antics	Acrònims nous	Durada	Suport
idCAT: ciutadà	idCAT	CPIXSA_C2	CPISA-2_idcat	4 anys	programari
T-CAT:certificats electrònics qualificats d'Empleat Públic	T-CAT	CPISRC_C1	CPI-1 + CPSQ-1	4 anys	targeta
	T-CATP	CPIXSA_C1	CPISA-1	4 anys	programari
	T-CAT Representant	N/A	CPRISQ-1	4 anys	targeta
	T-CAT pseudònim	N/A	CPPI-1 + CPPSQ-1	4 anys	targeta
T-CAT: Certificats electrònics qualificats de segell electrònic de l'administració pública	Segell nivell mig	CDANM-1	CDA-1_SGNM	3 anys	programari
T-CAT: Certificats aplicació	Dispositiu aplicacio	CDA-1	CDA-1	3 anys	programari
T-CAT: certificats de dispositiu	Dispositiu SSL	CDS-1	CDS-1	2 anys	programari
	Dispositiu SSL EV	CDSEV-1	CDSQ-1	2 anys	programari
	Seu-e nivell mig	CDS-1_SENM	CDS-1_SENM	2 anys	programari

#