



Catàleg de certificats de CATCert

Catàleg de certificats

CATCert

Agència Catalana
de Certificació



Índex

■ Què entenem per T-CAT	3
■ Per a què serveix	3
■ Qui emet certificats T-CAT	3
■ Quins certificats oferim	4
○ T-CAT (CPISR-1+CPX-1)	
○ T-CAT amb càrrec (CPISRC-1+CPXC-1)	
○ T-CAT d'operador d'entitat de registre T-CAT (CIPISR-1)	
○ T-CAT d'entitat en targeta (CEISR-1+CEX-1)	
○ T-CAT d'entitat en programari (CEIXSA-1)	
○ Certificat dispositiu servidor segur (CDS-1)	
○ Certificat dispositiu servidor segur <i>extended validation</i> (CDS-1 EV)	
○ Certificat de Seu electrònica <i>extended validation</i> (CDS-1 SENM EV i CDS-1 SENA EV)	
○ Certificat de dispositiu servidor de controlador de domini (CDSCD-1)	
○ Certificat d'aplicació (CDA-1)	
○ Certificat de Segell electrònic (CDA-1 SENM i CDA-1 SENA)	
○ Certificat de signatura de programari (CDP-1)	
■ Preus	8
■ Condicions del servei	9
○ Condicions de l'emissió/renovació de certificats	
○ Condicions de l'emissió/renovació urgent de certificats	
■ Altres productes	10
○ Certificats de proves	
○ Llicència dels certificats	



Què entenem per "T-CAT"

La **T-CAT** és la targeta del personal de les administracions públiques catalanes i conté certificats digitals de CATCert que permeten garantir la identitat i els atributs personals del seu titular.

Per a què serveix

La finalitat de la T-CAT és la de dotar al personal de l'administració d'una eina que els identifiqui en les comunicacions electròniques tot permetent signar documents en format electrònic per tal de fer possibles els tràmits i les consultes en línia amb tota garantia i agilitzant-ne les gestions.

Qui emet certificats T-CAT

L'emissió de certificats és una de les funcions de CATCert, adreçada a proveir de certificats digitals a les administracions públiques catalanes. També s'ofereix la renovació dels certificats des dels 60 dies previs a la caducitat, sent aquest un procés molt similar al d'emissió.

En el cas que hagueu xifrat algun document, haureu de conservar el certificat antic per poder recuperar el fitxer. O bé, desxifrar els documents amb l'antic i xifrar de nou amb el certificat obtingut.



Quins certificats oferim

■ T-CAT (CPISR-1+CPX-1)

El certificat personal en targeta va adreçat a persones físiques i disposa d'informació referent al titular que permet identificar-lo. 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.

Complementant aquest certificat, que es lliura en targeta per tal de garantir que generi signatura reconeguda, es lliura un certificat de xifrat que permet xifrar documents i rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text per part de l'emissor del missatge.

Tècnicament a CATCert es coneix aquesta parella de certificats lliurats en una mateixa targeta com a CPISR-1 i CPX-1, respectivament.

■ T-CAT amb càrrec (CPISRC-1+CPXC-1)

Aquest certificat té les mateixes prestacions que el certificat T-CAT (CPISR-1+CPX-1) però, a banda, permet identificar-se com a persona posseïdora d'un determinat càrrec. Se subministra conjuntament amb un certificat de xifrat.

Tècnicament a CATCert es coneix aquesta parella de certificats lliurats en una mateixa targeta com a CPISRC-1 i CPXC-1, respectivament.

■ 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 CATCert en l'emissió de certificats, requereixen certificats digitals per tal d'operar amb les seves aplicacions informàtiques.

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 la d'identificar els operadors que accedeixen a les aplicacions de l'ER T-CAT i permetre la signatura de les operacions realitzades.

Tècnicament a CATCert es coneix aquest certificat lliurat en targeta com a CIPISR-1.

■ T-CAT d'entitat en targeta (CEISR-1+CEX-1)

El certificat d'entitat en targeta va adreçat a persones jurídiques que volen nomenar a un representant per a certs tràmits o actes en que calen certificats digitals. D'aquesta forma, s'utilitzen en aplicacions que requereixen la identificació i/o signatura electrònica tot vinculant una persona física (NIF) a una organització (CIF) el que li permetrà realitzar certs tràmits en nom d'aquesta. Ex: Model 190 - Agència Tributària.

Complementant aquest certificat, que es lliura en targeta per tal de garantir que generi signatura reconeguda, es lliura un altre certificat de xifrat que garanteix la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permet xifrar documents i rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text per part de l'emissor del missatge.



Tècnicament a CATCert es coneix aquesta parella de certificats lliurats en una mateixa targeta com a CEISR-1 i CEX-1, respectivament.

Nota 1: aquest certificat no és vàlid per a la signatura de peticions d'emissió, renovació, habilitació o revocació de certificats.

Nota 2: CATCert no ofereix la recuperació de recuperació de claus d'aquest certificat.

■ T-CAT d'entitat en programari (CEIXSA-1)

El certificat d'entitat en programari també va adreçat a persones jurídiques i permeten que les entitats, és a dir, institucions, corporacions de dret públic i persones jurídico-públiques puguin signar missatges d'autenticació (confirmació de la identitat) i d'accés segur a sistemes informàtics; rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, utilitzant la clau pública del subscriptor i signar documents sense dispositiu segur de creació de signatura.

■ Certificat dispositiu servidor segur (CDS-1)

Quan es parla de servidors segurs sol referir-se a servidors web que fan servir un protocol de comunicacions que les protegeix i les fa més segures. És molt comú que els servidors web facin servir el protocol SSL (*Secure Sockets Layer*), que ofereix els següents serveis de seguretat:

- Identifica al servidor web davant l'usuari.
- Xifra les dades intercanviades entre l'usuari i el servidor.
- Pot identificar a l'usuari davant el servidor.

Els certificats de dispositiu servidor (CDS) de CATCert s'han d'instal·lar als servidors web de les administracions públiques catalanes. Així poden assegurar la seva identitat davant dels usuaris que s'hi connecten.

Poden, a més, garantir que el lloc web és l'original, el domini està registrat i 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.

■ Certificat dispositiu servidor segur *extended validation* (CDS-1 EV)

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

El principal avantatge és, un cop aconseguit el reconeixement amb Microsoft i Firefox, que els nous navegadors web els acceptaran immediatament i mostraran una confirmació de seguretat (imatge inferiors) que permetran als usuaris identificar

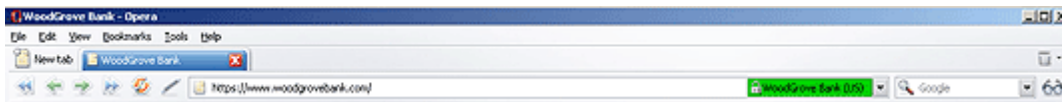


Catàleg de certificats de CATCert

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. Per exemple, Internet Explorer 7 mostra la barra d'adreces web en verd i el nom de l'organisme inclòs al certificat:



Confirmació de seguretat



Confirmació de seguretat de Mozilla Firefox

Per a més informació podeu visitar la pàgina del [CA/Browser Forum](#), organització sense ànim de lucre reguladora de l'estàndard i integrada pels principals prestadors de servei de certificació, proveïdors de navegadors d'Internet i empreses d'auditoria. També podeu consultar la descripció dels certificats EV que existeix a la [Wikipèdia](#).

■ Certificat de Seu electrònica *extended validation* (CDS-1 SENM EV i CDS-1 SENA EV)

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 la descriu l'article 10 de la Llei 11/2007, d'accés electrònic dels ciutadans als serveis públics.

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, CATCert emet el certificat de Seu tot seguint l'*Estàndard Extended Validation*, fet que garanteix el màxim nivell de seguretat en les transaccions que es realitzin en el lloc web que en faci ús. D'aquesta manera se substitueix l'anterior certificat de seu electrònica que queda suprimit del catàleg.

Podeu obtenir més informació a la descripció del certificat CDS EV (de la mateixa família que el certificats de Seu EV) d'aquest document, o en la web del [CA/Browser Forum](#), organització sense ànim de lucre reguladora de l'estàndard i integrada pels principals prestadors de servei de certificació, proveïdors de navegadors d'Internet i empreses d'auditoria. També podeu consultar la descripció dels certificats EV que existeix a la [Wikipèdia](#).

Aquest certificat es lliura en dos formats:

- **Seu electrònica de nivell mig *extended validation* (CDS-1 SENM EV):** el certificat, que es lliura en suport programari 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.
- **Seu electrònica de nivell alt *extended validation* (CDS-1 SENA EV):** el certificat de nivell alt és recomanable per a aquelles



administracions públiques que, havent realitzat prèviament una anàlisi de riscos, precisen mesures addicionals de seguretat, doncs contempen els següents riscos: infracció de seguretat, pèrdues econòmiques importants, pèrdua d'informació altament sensible i crítica o refutació d'una transacció amb impacte econòmic molt significatiu.

El certificat de nivell mig es lliurarà en suport programari i el de nivell alt s'haurà d'emmagatzemar en un HSM (maquinari criptogràfic) propietat del sol·licitant que compleixi les *Condicions tècniques per l'emissió de certificats de Seu i Segell de Nivell Alt* que trobareu a la web de CATCert (apartat més informació).

■ **Certificat de dispositiu servidor de controlador de domini (CDSCD-1)**

Aquest certificat permet als usuaris que pertanyen al domini de l'entitat autenticar-se amb certificat digital de signatura i xifrat en targeta, en una xarxa Windows. La autenticació consisteix en demostrar que el vostre certificat digital és original.

Tant els equips clients com els controladors de domini han d'estar configurats amb certificats vàlids i dominis registrats. Els controladors de domini han de tenir un certificat de controlador de domini per a poder autenticar usuaris amb targeta criptogràfica.

■ **Certificat d'aplicació (CDA-1)**

Aquest certificat s'emmagatzema en un servidor (preferiblement en un dispositiu criptogràfic) i pot ser requerit per una aplicació per signar un document o missatge.

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.

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

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.

■ **Certificat de Segell electrònic (CDA-1 SENM i CDA-1 SENA)**

És un certificat digital que serveix per a la identificació i l'autenticació de l'exercici de la competència en l'actuació administrativa automatitzada, en els termes descrits en l'article 18 de la Llei 11/2007, d'accés electrònic dels ciutadans als serveis públics.

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 es lliura en dos formats:

- **Segell electrònic de nivell mig (CDA-1 SENM):** el certificat de nivell mig, que es lliura en suport programari 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.



- **Segell electrònic de nivell alt (CDA-1 SENA):** el certificat de nivell alt és recomanable per a aquelles administracions públiques que, havent realitzat prèviament una anàlisi de riscos, precisen mesures addicionals de seguretat, doncs contempen els següents riscos: infracció de seguretat, pèrdues econòmiques importants, pèrdua d'informació altament sensible i crítica o refutació d'una transacció amb impacte econòmic molt significatiu.

El certificat de nivell mig es lliurarà en suport programari i el de nivell alt quedarà emmagatzemat al Signador Centralitzat de CATCert (consultar catàleg de serveis) o bé en un HSM (maquinari criptogràfic) propietat del sol·licitant que compleixi les *Condicions tècniques per l'emissió de certificats de Seu i Segell de Nivell Alt* que trobareu a la web de CATCert (apartat més informació).

■ Certificat de signatura de programari (CDP-1)

El certificat de dispositiu programari o de signatura d'aplicacions informàtiques serveix per signar electrònicament les aplicacions informàtiques o programari a transmetre a través d'Internet. Signant el codi d'una aplicació podem:

- Garantir-ne l'autoria. Això és, podem comprovar la identitat de l'organització que distribueix el codi mirant qui és el titular del certificat amb el que s'ha signat.
- Assegurar la integritat del codi, per estar segurs de que és lícit i no ha estat modificat de forma no autoritzada després d'haver-lo aprovat l'autor.

Les administracions públiques poden necessitar distribuir alguna peça de programari entre els usuaris (per exemple, penjant-lo d'una pàgina web) donant-ne garantia d'autenticitat. O potser necessiten assegurar el codi de les aplicacions que s'executen en els sistemes en prevenció de modificacions no autoritzades o errònies.

Aquests certificats poden ser personals o per a l'ens. És habitual signar codi com ara: Applets, scripts, executables, etc.

Preus:

■ Taula resum de característiques dels certificats personals

Nom del certificat	Acrònim	Funcions	Tipus de signatura	Suport	Mida de claus en bits	Durada en anys	Cost sense IVA (18%)*
T-CAT	CPISR-1+ CPX-1	·Signatura ·Xifrat ·Identificació	Signatura reconeguda	Targeta criptogràfica	2.048	4	24 €
T-CAT amb càrrec	CPISRC-1+ CPXC-1	·Signatura ·Xifrat ·Identificació	Signatura reconeguda	Targeta criptogràfica	2.048	4	24 €
T-CAT d'operador d'ER T-CAT	CIPIISR-1	·Signatura ·Identificació	Signatura reconeguda	Targeta criptogràfica	2.048	4	24 €

* Consulteu les *Condicions del servei* d'aquest document



■ Taula resum de característiques dels certificats d'entitat

Nom del certificat	Acrònim	Funcions	Tipus de signatura	Suport	Mida de claus en bits	Durada en anys	Cost sense IVA (18%)*
T-CAT d'entitat en targeta	CEISR-1+ CEX-1	·Signatura ·Xifrat ·Identificació	Signatura reconeguda	Targeta criptogràfica	2.048	4	24 €
T-CAT d'entitat en programari	CEIXSA	·Signatura ·Xifrat ·Identificació	Signatura avançada	Programari	2.048	4	24 €

* Consulteu les *Condicions del servei* d'aquest document

■ Taula resum dels certificats de dispositiu

Nom del certificat	Acrònim	Tipus de signatura	Suport	Mida de claus en bits	Durada en anys	Cost sense IVA (18%)*
Dispositiu servidor segur	CDS-1	Autenticació SSL	Programari	2.048	2	43 €
Dispositiu servidor segur EV**	CDS-1 EV	Autenticació SSL	Programari	2.048	2	125 €
Seu electrònica de nivell mig EV**	CDS-1 SENM EV	Autenticació SSL	Programari	2.048	2	125 €
Seu electrònica de nivell alt EV**	CDS-1 SENA EV	Autenticació SSL	Programari per a HSM	2.048	2	700 €
Dispositiu servidor de controlador de domini	CDSCD-1	Autenticació domini Windows	Programari	2.048	2	43 €
Certificat d'aplicació	CDA-1	Signatura automatitzada nivell mig	Programari	2.048	4	43 €
Segell electrònic de nivell mig	CDA-1 SENM	Signatura automatitzada nivell mig	Programari	2.048	3	125 €
Segell electrònic de nivell alt**	CDA-1 SENA	Signatura automatitzada nivell alt	Programari per a HSM	2.048	3	700 €
Signatura de programari	CDP-1	Autenticació de codi	Programari	2.048	4	43 €

* Consulteu les *Condicions del servei* d'aquest document

** Degut als estrictes requisits de seguretat aquest certificats només podran ser sol·licitats a l'Entitat de Registre de CATCert mitjançant el procediment habitual.

Condicions del servei

■ **Condicions de l'emissió/renovació de certificats**

1. El servei ordinari d'emissió de certificats es compromet a lliurar els certificats en 16 dies laborables comptats a partir de la recepció de la documentació de sol·licitud correctament emplenada i signada.



2. Els costos indicats en les taules resum de cada tipus de certificat són preus establerts per a aquells ens que no poden constituir-se com a entitat de registre T-CAT. En cas de complir els criteris per ser-ho, si l'ens s'estima més sol·licitar els certificats a CATCert, el preu serà el triple de l'indicat en aquestes tarifes.

El criteri per tal de ser ER T-CAT és complir dos o més dels requisits indicats a continuació:

- Ser un ens supramunicipal
 - Tenir més de 50.000 habitants en el seu àmbit territorial
 - Tenir usos disponibles amb certificat digital per als treballadors de l'ens
 - Tenir més de 200 certificats digitals dins de l'ens o tenir-los previstos per al període d'un any
3. El cinc primers certificats vigents, personals o d'entitat, seran gratuïts. És a dir, aquells ens que en total tinguin cinc o menys certificats vigents (sumant els personals i els d'entitat) en el moment de la sol·licitud, no hauran de pagar cap fins que demanin el sisè.
 4. El cinc primers certificats de dispositiu vigents seran gratuïts. És a dir, aquells ens que en total tinguin cinc o menys certificats de dispositiu vigents en el moment de la sol·licitud, no hauran de pagar cap fins que demanin el sisè.

■ Condicions de l'emissió/renovació urgent de certificats

CATCert posa a disposició dels seus usuaris un servei d'emissió i renovació urgent de certificats per a tots aquells que, per motius d'urgència no puguin esperar al termini ordinari de 16 dies laborables. Donada la naturalesa del servei, aquest es limita a cinc certificats per ens i setmana que es lliuraran en un termini màxim de 4 dies laborables comptats a partir de la recepció correcta de la sol·licitud.

Tipus de certificat	Cost sense IVA (18%)
Certificats personals	El doble del preu ordinari
Certificats d'entitat	
Certificats de dispositiu	

Altres productes

■ Certificats de proves

S'ofereixen dos tipus de certificats de proves: amb dades genèriques i amb dades personalitzades:

- Certificats amb dades genèriques: els certificats han estat emesos per les entitats de certificació de CATCert i contenen dades fictícies com "organització de proves" o "nom cognom cognom". No es poden personalitzar i són gratuïts. Només cal demanar-los al CAU de CATCert. Es lliura un paquet complet per cada EC que es demani, amb tots els certificats del catàleg de CATCert en estat vàlid, revocat i caducat.



- Certificats amb dades personalitzades: si l'usuari necessita certificats amb dades concretes, CATCert ofereix aquest servei però els certificats generats ho seran des de les EC de preproducció (entorn fictici de proves). Això és degut a que, si es fessin en l'entorn real serien certificats plenament vàlids i amb possibles dades reals, fet que suposaria una violació de la normativa d'emissió de CATCert.

Separadament, si l'usuari ho requereix, CATCert subministrarà targetes verges per a carregar els certificats (aquesta feina haurà de ser assumida per l'usuari), tot i que es poden reutilitzar targetes que tingui l'usuari amb certificats caducats o revocats.

Concepte	Suport en que es lliuren	EC emissora	Cost sense IVA (18%)
Certificats amb dades genèriques (tots els perfils en estat vàlid, revocat i caducat)	Programari	Qualsevol EC real de CATCert (Producció)	0 €
Certificats amb dades personalitzades (tots els perfils en estat vàlid)	Els mateixos que en el cas dels certificats reals	Qualsevol EC simulada de CATCert (Preproducció)	11 €/certificat
Targeta verge CATCert	-	-	8 €

■ Llicència dels certificats


Aquestes tarifes afecten només a certs projectes en que es facturen les llicències dels certificats per separat. Per defecte, tots els certificats digitals que emet CATCert inclouen el cost de la llicència.

Tipus de certificat	Cost sense IVA (18%) *
Certificats en targeta	1.45 € (1€ de la llicència anual + 0.45 del manteniment dels tres següents anys)
Certificats de programari	7.25€ (5€ de la llicència anual + 2.25 del manteniment dels tres següents anys)

* Els preus dels certificats dels apartats anteriors ja inclouen el preu de la llicència i el manteniment



Control documental

Estat formal	Elaborat per: Equip CATCert	Aprovat per: Consell d'Administració de CATCert
Data de creació	27/07/2011	
Control de versions	Data:	30/11/2011
	Descripció:	Actualització de les tarifes amb els certificats <i>extended validation</i> i nivell alt.
Nivell accés informació	pública	
Títol	Catàleg de certificats de CATCert	
Control de còpies	Només les còpies disponibles al web de CATCert garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.	
Drets d'autor	 <p>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 http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.</p>	