



Agència Catalana
de Certificació



Consorci
Administració Oberta
de Catalunya

CONDICIONS GENERALS D'ÚS

APLICABLES A

CERTIFICATS DE DISPOSITIU DE SERVIDOR SEGUR (CDS)

(CDS-1 Seu electrònica)

t del

Control documental

Estat formal	Elaborat per: Carlos Alonso	Aprovat per: Marta Cruellas
Data de creació	14/07/2009	
Control de versions	Data:	
	Descripció:	Aprofundiment en els casos de responsabilitat i homogeneïtzació de les CGU
Nivell d'informació accés	pública	
Títol	Condicions Generals d'Ús del Certificat de Dispositiu Servidor Segur CDS-1 Seu Electrònica	
Fitxer	D1111 N-CGU CDS-1 Seu electrònica v2r3 cat	
Control de còpies	Només les còpies disponibles a https://www.catcert.cat/ 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 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.	

CONDICIONS GENERALS D'ÚS

APLICABLES A

CERTIFICATS DE DISPOSITIU DE SERVIDOR SEGUR (CDS)

(CDS-1 Seu electrònica)

Abans de verificar un certificat electrònic de dispositiu de servidor segur per a Seu Electrònica¹ (en endavant, "CDS-1 Seu electrònica"), d'acord amb la Llei 11/2007, de 22 de juny, d'Accés Electrònic dels Ciutadans als Serveis Públics, o d'accedir o utilitzar la informació de l'estat de certificats i la resta de informació continguda en el Registre de CATCert, Vostè (en endavant, "el Verificador") ha de llegir i acceptar les presents Condicions Generals d'Ús (en endavant, "Condicions d'Ús").

La realització de qualsevol de les accions descrites en el paràgraf anterior implicarà que s'han acceptat, en la seva totalitat, les presents Condicions d'Ús.

Les condicions d'emissió del CDS-1 Seu electrònica, aplicables al subscriptor o al posseïdor de claus del certificat, es troben regulades en les "Condicions Generals d'Emissió" de CATCert aplicables.

En el supòsit que el Verificador no estigui conforme amb la totalitat dels termes de les presents Condicions d'Ús haurà d'abstenir-se de realitzar qualsevol acció que guardi relació amb les clàusules aquí contingudes. En aquest cas, CATCert no assumeix responsabilitat alguna.

CLÀUSULES

PRIMERA.- Objecte

1.- Les presents Condicions d'Ús regulen la prestació per CATCert dels serveis de informació sobre els certificats, l'estat dels certificats i altres informacions publicades en el Registre de CATCert, en relació amb els certificats descrits en la clàusula tercera d'aquestes Condicions d'Ús.

2.- Aquestes Condicions d'Ús proporcionen garanties limitades al servei ofert, exclouent qualsevol altra garantia i responsabilitat que no derivi del servei de certificació ofert al Verificador.

SEGONA.- DPC i documentació d'operacions de CATCert

1. La prestació dels Serveis de Certificació de CATCert es regula tècnica i operativament a la Declaració de Pràctiques de Certificació de CATCert (en endavant, la DPC) i les seves actualitzacions posteriors, així com en la documentació complementària publicada en compliment del que disposen els articles 18 i 19 de la

¹ La seu electrònica és aquella adreça electrònica disponible per als ciutadans a través de xarxes de telecomunicacions la titularitat de les quals, gestió i administració correspon a una Administració Pública, òrgan o entitat administrativa en l'exercici de les seves competències.

Llei 59/2003, de 19 de desembre, sobre signatura electrònica, en la següent adreça d'Internet: <http://www.catcert.net/registre>.

2. La DPC i la documentació d'operacions de CATCert, modificades periòdicament, s'incorporen a les presents Condicions d'Ús per referència. El Verificador declara conèixer la última versió de la DPC, els aspectes jurídics de la qual es contenen en les presents Condicions d'Ús.

3. El Verificador es compromet a complir amb els requisits tècnics, operatius i de seguretat descrits en la DPC i en la documentació d'operacions de CATCert.

4. En cas de discrepància, el significat dels termes continguts en les presents Condicions d'Ús prevaldrà sobre allò establert en la DPC.

TERCERA.- *Descripció del CDS-1 Seu electrònica*

3.1. Naturalesa del Certificat

Els CDS-1 Seu electrònica són certificats de dispositiu caracteritzats pel fet que el posseïdor de la clau privada és un dispositiu informàtic que realitza operacions de signatura i xifrat de forma automàtica, sota la responsabilitat del subscriptor.

Els CDS-1 Seu electrònica són certificats destinats a ser utilitzats per una aplicació informàtica, servidor SSL o de TLS, per tal que s'identifiqui davant les aplicacions client que s'hi connectin i per protegir el secret de les comunicacions entre el client i el servidor.

Els CDS-1 Seu electrònica són certificats reconeguts, tal i com preceptua l'article 11 de la Llei 59/2003, de 19 de novembre, de Signatura Electrònica.

3.2. Finalitat i usos del Certificat

Els CDS-1 Seu electrònica permeten garantir la identitat de la Seu Electrònica i dels servidors concrets on funcionen així com l'establiment amb ella de comunicacions segures, des del moment en què s'ha obtingut un certificat vàlid i mentre aquest es trobi vigent.

Els CDS-1 Seu electrònica són emesos per una Entitat de Certificació de la jerarquia pública de certificació de Catalunya, per a l'ús indicat en el paràgraf anterior.

Els CDS-1 Seu electrònica s'identifiquen amb l'identificador d'objecte (OID):

Nivell mig: 1.3.6.1.4.1.15096.1.3.1.51.2

Nivell alt: 1.3.6.1.4.1.15096.1.3.1.51.3

QUARTA.- *Llicència d'ús del Certificat*

4.1. Reserva de drets

Tots els continguts accessibles en relació amb la prestació dels serveis de certificació, el propi CDS-1 Seu electrònica, així com les especificacions, targetes, marques i altres aplicatius aparellats al seu ús estan subjectes a drets de propietat intel·lectual i industrial de CATCert o d'altres tercers titulars d'aquests.

En cap cas la prestació d'aquests serveis implica cap tipus de renúncia, transmissió o cessió total o parcial d'altres drets que els expressament reconeguts i atorgats en les presents Condicions d'Ús.

4.2. Llicència d'ús del CDS-1 Seu electrònica

CATCert atorga al Verificador llicència d'ús no exclusiva e intransferible del CDS-1 Seu electrònica i de la informació d'estat d'aquests, amb la única i exclusiva finalitat de prestar-li els serveis i permetre l'ús del certificat de conformitat amb les presents Condicions d'Ús.

4.3. Inexistència de garantia de idoneïtat

CATCert no pot garantir que la utilització del CDS-1 Seu electrònica i aplicatius informàtics aparellats permeti al Verificador l'obtenció o cobertura de necessitats, dades o fins de qualsevol índole, diferents als que poden assolir-se mitjançant el seu ús segons la seva pròpia naturalesa i segons el que es desprèn de la seva llicència d'ús.

4.4. Limitacions d'ús i usos prohibits

El CDS-1 Seu electrònica només podrà ser utilitzat dins dels límits d'ús recollits de manera expressa a la seva llicència d'ús i en les presents Condicions d'Ús. Qualsevol altre ús fora dels descrits en la present clàusula queden expressament exclosos del present àmbit contractual i formalment prohibits.

El certificat no s'ha dissenyat, no es pot destinar i no s'autoritza el seu ús o revenda amb equips de control de situacions perilloses o per a usos que requereixen actuacions a prova d'errors, amb el funcionament de instal·lacions nuclears, sistemes de navegació o comunicacions aèries, o sistemes de control d'armament, on un error pogués directament comportar la mort, lesions personals o danys mediambientals severes.

4.5. Duració de la llicència

La duració de la llicència d'ús del CDS-1 Seu electrònica està limitada al termini màxim de validesa d'aquest, que és d'un (1) any.

La data d'inici de la vigència dels certificats ve determinada pel dia de la seva emissió, mentre que de la seva expiració figura indicada en el propi certificat, més enllà de qual no podrà utilitzar-se.

CINQUENA.- Obligacions del Verificador

5.1. Decisió informada

CATCert informa al Verificador, el qual es dóna per notificat, que té accés a informació suficient per prendre una decisió informada en el moment de verificar un CDS-1 Seu electrònica i confiar en la informació continguda en aquest.

De la mateixa forma, el Verificador reconeix que l'ús del Registre i de les Llistes de Revocació de Certificats (en endavant, "les LRCs" o "les CRLs") de CATCert, es regeix per la DPC de CATCert i es compromet a complir els requisits tècnics, operatius i de seguretat descrits en l'esmentada DPC de CATCert.

5.2. Requisits de verificació de signatures electròniques

Per confiar en una signatura electrònica, és imprescindible que el Verificador comprovi l'existència i la validesa tant del certificat com de la signatura electrònica, mitjançant l'execució del procediment de verificació.

La verificació implica comprovar l'autenticitat i la integritat del document electrònic signat, a fi de determinar que va ser generada per la EC legítima, que és la Agència Catalana de Certificació, utilitzant la clau privada corresponent a la clau pública continguda en el certificat del subscriptor, i que el document no va ser modificat des de la generació de la signatura electrònica.

La comprovació del certificat serà executada normalment de forma automàtica pel programari del Verificador i, en tot cas, de conformitat amb la DPC, amb els següents requisits ineludibles:

- a) Utilitzar el programari apropiat per a la verificació de la signatura electrònica del CDS-1 Seu electrònica amb els algorismes i longituds de claus autoritzats en el certificat i/o executar qualsevol altra operació criptogràfica, i establir la cadena de certificats en què es basa la signatura electrònica a verificar, ja que la signatura electrònica es verifica utilitzant aquesta cadena de certificats.
- b) Assegurar que la cadena de certificats identificada és la més adequada per a la signatura electrònica que es verifica, ja que una signatura electrònica pot basar-se en més d'una cadena de certificats, i és decisió del Verificador assegurar-se d'utilitzar la cadena més adequada per verificar-la.
- c) Comprovar l'estat de revocació dels certificats de la cadena amb la informació subministrada en el Registre de CATCert (Per exemple, la continguda en les LRCs) per determinar la validesa de tots els certificats de la cadena de certificats, doncs només pot considerar-se correctament verificada una signatura electrònica si tots i cada un dels certificats de la cadena són correctes i es troben vigents.
- d) Assegurar que tots els certificats de la cadena autoritzen l'ús de la clau privada pel subscriptor del certificat i el posseïdor de la clau, degut a la possibilitat de que algun dels certificats inclogui límits d'ús que impedeixin confiar en la signatura electrònica que es verifica. Cada certificat de la cadena disposa d'un indicador que fa referència a les Condicions d'Ús aplicables, per a la seva revisió pels Verificadors.

- e) Verificar tècnicament la signatura de tots els Certificats de la cadena abans de confiar en el Certificat utilitzat pel signatari.
- f) Determinar la data i l'hora de generació de la signatura electrònica, ja que la signatura electrònica només pot considerar-se correctament verificada si ha estat creada dins el període de vigència de la cadena de certificats en què es basa.
- g) Delimitar les dades que han estat signades digitalment, ja que aquestes s'utilitzaran en la verificació de la signatura.
- h) Verificar tècnicament la pròpia signatura amb el certificat del signatari avalat per la cadena de certificats.

5.3. Diligència exigible

El Verificador ha d'actuar amb la màxima diligència abans de confiar en un CDS-1 Seu electrònica. En concret, el Verificador s'obliga a utilitzar el programari de verificació de signatura electrònica amb la capacitat tècnica, operativa i de seguretat suficient per executar el procés de verificació de signatura correctament, i serà responsable exclusiu del dany que pugui sofrir per la incorrecta elecció de l'esmentat programari.

La prescripció anterior no serà aplicable quan CATCert hagi subministrat el programari de verificació al Verificador.

El Verificador pot confiar en un CDS-1 Seu electrònica si concorren les condicions següents:

- a) La signatura electrònica s'ha de poder verificar d'acord amb els requisits establerts en l'apartat segon de la clàusula cinquena.
- b) El Verificador ha d'haver utilitzat informació de revocació actualitzada en el moment de verificar la firma.
- c) El tipus i la classe de certificat ha de ser l'apropiat per a l'ús que es pretén fer.
- d) El Verificador ha de tenir en compte altres limitacions addicionals d'ús del certificat, indicades de qualsevol forma en el certificat, incloent aquelles no processades automàticament pel programari de verificació, incorporades per referència al certificat, i contingudes en aquestes Condicions d'Ús. En especial, un certificat no constitueix una concessió de drets i facultats per part de CATCert al subscriptor o al posseïdor de claus, més enllà de la descripció del certificat segons la clàusula tercera o una altra indicació expressa de CATCert o del propi subscriptor.
- e) Finalment, la confiança ha de ser raonable d'acord amb les circumstàncies. Si les circumstàncies requereixen garanties addicionals, el Verificador haurà d'obtenir aquestes garanties per tal que la confiança sigui raonable.

En qualsevol cas, la decisió final respecte a confiar o no en un certificat CDS-1 Seu electrònica verificat és exclusivament del Verificador, qui ha d'adoptar una actitud activa i al que se li exigeix l'accés a tota la informació disposada per CATCert per a prendre les seves decisions de forma totalment informada. En cas de dubte, el Verificador no ha de confiar en el CDS-1 Seu electrònica.

5.4. Confiança en una signatura no verificada

Queda prohibit confiar, o, de qualsevol altra forma, fer ús d'una signatura o certificat no verificats.

Si el Verificador confia en un certificat no verificat, assumirà tots els riscos derivats d'aquesta actuació.

5.5. Efecte de la verificació

En virtut de la correcta verificació d'una signatura i/o certificat CDS-1 Seu electrònica, de conformitat amb les Condicions d'Ús, el Verificador pot confiar en les dades del certificat o la LRC, dins de les limitacions d'ús corresponents.

5.6. Ús correcte i activitats prohibides

El Verificador s'obliga a no utilitzar cap classe d'informació d'estat dels certificats o de cap altre tipus que hagi estat subministrada per CATCert, en la realització de qualsevol acte prohibit per la llei aplicable a aquest.

El Verificador s'obliga a no inspeccionar, interferir o realitzar enginyeria inversa en la implantació tècnica dels Serveis Públics de Certificació de CATCert, sense previ consentiment escrit de CATCert.

Adicionalment, el Verificador s'obliga a no comprometre intencionadament la seguretat dels Serveis Públics de Certificació de CATCert.

Els serveis de certificació digital prestats per CATCert no han estat dissenyats ni permeten la utilització o revenda, com equips de control de situacions perilloses o per a usos que requereixen actuacions a prova d'errors, com l'operació de instal·lacions nuclears, sistemes de navegació o comunicació aèria, sistemes de control de tràfic aeri, o sistemes de control d'armament, on un error podria causar la mort, danys físics o danys mediambientals greus.

SISENA.- Obligacions de CATCert

6.1. Relatives a la Prestació del Servei de Verificació de Certificats

CATCert s'obliga a la prestació del servei en determinades condicions tècniques i operatives, tal i com s'estableix en la DPC de CATCert, incloent un Registre de certificats, on es publica informació relativa a l'estat dels certificats.

CATCert s'obliga a emetre informació d'estat, incloent la suspensió i la revocació, dels certificats emesos, d'acord amb la DPC, així com a assumir les seves responsabilitats davant dels verificadores, sempre dins dels límits d'ús establerts pels certificats.

6.2. Garantia limitada de CATCert

CATCert garanteix al Verificador les condicions del servei següents:

- a) El Certificat CDS-1 Seu electrònica conté informació correcta i actual en el moment de la seva emissió, degudament comprovada.
- b) El Certificat CDS-1 Seu electrònica compleix tots els requisits relatius al contingut i al format establert a la DPC.
- c) La clau privada de CATCert no ha estat compromesa, excepte notificació en contra mitjançant el Registre.

SETENA.- Règim de Responsabilitats

7.1. Responsabilitat del Verificador

El Verificador respondrà per incompliment de les seves obligacions contractuals o per negligència.

El Verificador s'obliga a mantenir a CATCert indemne de qualsevol acte o omissió de la que resultin danys de tot tipus, incloent:

- a) L'incompliment de les obligacions pròpies del Verificador.
- b) La confiança en un certificat o signatura electrònica basada en aquest, que no sigui raonable.
- c) L'incompliment de l'obligació de comprovar l'estat d'un certificat per a determinar si ha expirat o ha estat suspès o revocat.

7.2. Responsabilitat de CATCert

CATCert respondrà per incompliment de les obligacions que, en cada cas, imposa la Llei 59/2003, de 19 de desembre, sobre signatura electrònica o per negligència, excepte en els casos següents:

- a) CATCert no serà responsable pels danys causats per les informacions contingudes en els certificats, sempre que aquestes siguin correctes i actuals en el moment de la emissió del certificat.
- b) CATCert no serà responsable de cap dany directe o indirecte, especial, incidental, emergent, de qualsevol lucre cessant, pèrdua de dades, danys punibles, previsibles o imprevisibles, derivats de l'ús, enviament, llicència a tercers, funcionament o no funcionament dels certificats en un sistema no proporcionat per CATCert, així com de les signatures digitals o qualsevol altra

transacció o servei descrit en la DPC, quan siguin utilitzats fora del Servei Públic de Certificació i els serveis de verificació de CATCert.

- c) L'Entitat de Certificació no serà en cap cas responsable de cap dany que resulti de cas fortuit o força major, com ara desastres naturals o disfuncions generals de les xarxes de telecomunicacions i solucions tecnològiques el funcionament de les quals no siguin responsabilitat de l' Entitat de Certificació.
- d) L'Entitat de Certificació no respondrà dels danys o perjudicis derivats de l'acció d'un tercer.
- e) L'Entitat de Certificació no serà responsable dels danys o perjudicis que pugui causar l'aplicació de normes legislatives o reglamentàries aprovades amb posterioritat a l'emissió d'aquestes Condicions Generals.

VUITENA.- Infracció de drets de tercers

CATCert no es responsabilitza de què l'enviament a CATCert, pel subscriptor o pel posseïdor de claus, per a la seva inclusió al certificat, així com la utilització d'un nom de domini i/o qualsevol altre tipus de nom o denominació, i la resta d'informació de sol·licitud dels certificats, infringeixi els drets de persona alguna en qualsevol jurisdicció respecte a les seves marques registrades, marques de servei, noms comercials o qualsevol altre dret de propietat intel·lectual o industrial, ni de què el subscriptor o el posseïdor de claus pretengui utilitzar el domini i els nom distingits per a cap propòsit il·legal, incloent-hi, sense limitació, la infracció amb dol d'un contracte, o l'obtenció de possibles avantatges comercials, la competència deslleial, la lesió del dret a l'honor, i la confusió o engany d'una persona, tant física com jurídica.

CATCert no es responsabilitza de la veracitat de la informació que li hagi estat comunicada pel subscriptor o pel posseïdor de claus, per a la seva inclusió als certificats emesos per CATCert, en jurisdicció qualsevol en la que aquesta informació es pugui utilitzar o visualitzar.

NOVENA.- Protecció de dades personals

Determinades informacions relatives als certificats contenen dades de caràcter personal que han de protegir-se en atenció al que preceptua la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

El Verificador s'obliga a protegir les esmentades dades personals, així com a establir les adequades mesures de seguretat, de conformitat amb l'article 9 de la citada Llei Orgànica 15/1999.

En cas de què el Verificador rebi de l'Entitat de Certificació qualsevol tipus de informació de caràcter personal en execució de les presents Condicions d'Ús, es compromet a utilitzar-la amb l'exclusiva finalitat de verificar la signatura del subscriptor

del certificat. Així mateix, s'obliga a no utilitzar aquestes dades per a qualsevol altre fi, sense el consentiment exprés del subscriptor.

El Verificador serà responsable exclusiu de les incidències derivades de la infracció d'aquestes obligacions de protecció de dades personals, obligant-se a mantenir indemne a l'Entitat de Certificació de tot dany derivat d'aquestes incidències.

DESENA.- *Divisibilitat de les Condicions d'Ús*

Les clàusules de les presents Condicions d'Ús són independents entre sí, motiu pel qual si qualsevol clàusula es considerada invàlida o inaplicable, la resta de clàusules de les presents Condicions d'Ús seguiran sent aplicables, excepte acord exprés en contrari de les parts.

ONZENA.- *Finalització de la relació jurídica i supervivència de determinades obligacions*

Aquestes Condicions d'ús finalitzaran quan acabi la llicència d'ús del certificat que es concedeix, i de forma anticipada per infracció, per qualsevol de les parts, de les seves obligacions establertes en la Declaració de Pràctiques de Certificació.

Les següents obligacions de la Declaració de Pràctiques de Certificació romandran vigents per ambdues parts durant un termini màxim de dos anys des de la finalització d'aquest contracte: Obligacions i responsabilitat civil (secció 9.6 de la DPC), auditoria de conformitat (secció 8 de la DPC), i confidencialitat (9.4). Les obligacions derivades de la protecció de dades personals romandran mentre no es cancel·lin les dades personals, d'acord amb la normativa vigent.

DOTZENA.- *Notificació*

Totes les modificacions que l'Entitat de Certificació realitzi sobre aquestes condicions generals seran notificades a través de la pàgina web de l'Entitat de Certificació indicada a la clàusula segona d'aquestes condicions generals.

El verificador ha de remetre qualsevol notificació en relació amb aquestes condicions generals a les adreces de l'Entitat de Certificació indicades a la pàgina web de l'Entitat de Certificació.

TRETZENA.- *Legislació aplicable i jurisdicció competent*

Les presents Condicions d'ús seran interpretades i executades en els seus propis termes i, en tot allò no previst, les parts es regiran per la Llei 59/2003, de 19 de desembre, per la legislació administrativa aplicable i, subsidiàriament, per la legislació civil i mercantil que regula el règim de les obligacions i dels contractes.

La jurisdicció competent és la que s'indica en la Llei 29/1998, de 13 de juliol, reguladora de la Jurisdicció Contenciosa Administrativa.