Agència Catalana
de Certificació

Certificat de Dispositiu de Servidor Segur (CDS)

Referència:	D1111_E0650_N-TD CDS
Versió:	1.0
Data:	18/09/2006

Índex

1. INTRODUCCIÓ I INFORMACIÓ DE CONTACTE

1.1. Introducció

El present document és un simple text divulgatiu que té per finalitat difondre els aspectes fonamentals continguts en la Declaració de Pràctiques de Certificació (en endavant, DPC) i Política de Certificació (en endavant, PdC) de l'Agència Catalana de Certificació (en endavant, CATCert) en relació amb el Certificat de Dispositiu de Servidor Segur (CDS) no entenent-se, en cap cas, que desenvolupa, amplia o modifica la citada DPC i PdC de CATCert.

El present Text de Divulgació es troba subjecte a la jerarquia documental que es dedueix de la clàusula set del present document; jerarquia que haurà de ser respectada i que, en tot cas, resultarà d'aplicació.

1.2. Organització responsable

CATCert - Agencia Catalana de Certificació

Passatge de la Concepció, 11

08008 - Barcelona

1.3. Dades de contacte de l'organització

Per a qualsevol consulta, dirigeixin-se a:

CATCert - Agencia Catalana de Certificació

Àrea d'assessorament i recerca

Passatge de la Concepció, 11

08008 - Barcelona

2. TIPUS I FINALITAT DEL CERTIFICAT CDS

2.1. Certificat de Dispositiu de Servidor Segur (CDS)

Els CDS són certificats de dispositiu caracteritzats pel fet de què 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 són certificats destinats a ser utilitzats per una aplicació informàtica, servidor SSL o de TLS, per a què 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 són certificats ordinaris que garanteixen la identitat de la persona responsable i dels servidors concrets on funcionen.

Els certificats CDS s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.51

La duració de la llicència dels CDS és de quatre (4) anys, a comptar des de la data de la seva emissió.

2.2. Entitat de Certificació emissora

Els certificats CDS són emesos per una Entitat de Certificació pertanyent a la jerarquia pública de certificació de Catalunya.

3. LÍMITS D'ÚS

Els certificats s'utilitzaran de conformitat amb la seva funció pròpia i finalitat establerta, sense que pugui utilitzar-se en altres funciones i amb altres finalitats. De la mateixa forma, els certificats han d'utilitzar-se únicament d'acord amb la llei aplicable, especialment tenint en compte les restriccions de importació i exportació existents en cada moment.

L'extensió Key Usage s'utilitzarà per establir límits tècnics als usos que es pot donar a una clau privada corresponent a una clau pública llistada en un certificat X.509v3. Ha de tenir-se en compte que l'efectivitat de les limitacions basades en extensions de certificats depèn en ocasions de l'operació d'aplicacions informàtiques que no han estat fabricades ni poden ser controlades per CATCert.

Els certificats no s'han dissenyat, ni poden destinar-se i no s'autoritza el seu ús o revenda com equips de control de situacions perilloses o per a usos que requereixen actuacions a prova d'errors, com el funcionament de instal·lacions nuclears, sistemes de navegació o comunicacions aèries o sistemes d'armament, on un error pogués directament comportar la mort, lesions personals o danys mediambientals severs.

3.1. Límits d'ús dirigits als subscriptors

El subscriptor té que utilitzar el servei de certificació digital prestat per CATCert exclusivament per als usos autoritzats en el "Conveni de Col·laboració de Serveis de Certificació" que es reprodueixen de mode succint en la clàusula quarta del present Text de Divulgació.

Així mateix, el subscriptor s'obliga a utilitzar el servei de certificació digital d'acord amb les instruccions, manuals o procediments subministrats per CATCert.

El subscriptor ha de complir qualsevol llei i regulació que pugui afectar al seu dret d'ús de les eines criptogràfiques que utilitzi.

El subscriptor no pot adoptar mesures de inspecció, alteració o enginyeria inversa dels serveis de certificació digital de CATCert, sense previ permís exprés i per escrit de CATCert.

3.2. Advertències d'ús dirigides als verificadors

El Verificador dels certificats CDS ha d'utilitzar el servei de informació, prestat per CATCert, exclusivament per als usos autoritzats en les "Condicions Generales d'ús del Certificat CDS", que se reprodueixen concisament en la clàusula cinquena del present document.

De la mateixa forma, el Verificador s'obliga a utilitzar el servei de informació d'acord amb les instruccions, manuals o procediment subministrats per CATCert.

El Verificador ha de complir qualsevol llei i regulació que pugui afectar al seu dret a utilitzar les eines criptogràfiques que utilitzi.

El Verificador no pot adoptar mesures de inspecció, alteració o enginyeria inversa dels serveis de certificació digital de CATCert, sense previ permís exprés i per escrit d'aquest.

4. OBLIGACIONS DELS SUBSCRIPTORS

4.1. Sol·licitud del certificat i generació de claus

Abans de l'emissió i entrega d'un certificat, ha d'existir una sol·licitud de certificat.

La sol·licitud d'emissió d'un certificat CDS implica l'autorització del subscriptor a CATCert per a què generi les seves claus, privada i pública, per a la identificació i la signatura electrònica dins d'un dispositiu segur de creació de signatura electrònica (que s'entrega al posseïdor de claus) i per a què emeti el corresponent certificat.

El subscriptor s'obliga a realitzar la sol·licitud del certificat atenent:

- a les especificacions previstes per al certificat CDS,
- al procediment previst en la DPC i en la documentació d'operacions de CATCert, i
- als components tècnics subministrats per aquest, de ser necessaris.

4.2. Veracitat de la informació

El subscriptor se responsabilitza de què tota la informació inclosa, per qualsevol mitjà, en la sol·licitud del certificat i en el certificat sigui exacta, completa per a la finalitat del certificat i estigui actualitzada en tot moment.

El subscriptor té que informar immediatament a CATCert de qualsevol inexactitud en el certificat detectada una vegada emès, així com dels canvis que es produeixin en la informació aportada i/o registrada per a l'emissió del certificat.

En cas de què el posseïdor de claus cessi en la seva vinculació amb el subscriptor, aquest ha de sol·licitar immediatament la revocació del certificat.

4.3. Entrega i acceptació del servei

Amb la signatura de la fulla d'entrega, el subscriptor i, en el seu caso, el posseïdor de claus reconeix que se li ha entregat la targeta, el certificat, la clau privada i qualsevol altre suport tècnic entregat CATCert, així com, quan procedeixi, el codi de identificació personal. Així mateix, reconeixerà que aquests elements funcionen correctament.

El subscriptor i, en el seu caso, el posseïdor de claus accepta, amb la signatura de la fulla d'entrega o mitjançant el procediment telemàtic d'acceptació de certificats, el certificat CDS, segons s'especifica en la DPC de CATCert.

El subscriptor ha de gestionar la signatura de la fulla d'entrega de posseïdor de claus i ha de custodiar-la durant un període de quinze (15) anys, quedant tota la informació a disposició de CATCert, excepte quan l'activació del certificat es realitzi per mitjans telemàtics.

4.4. Posseïdor de claus

El subscriptor s'obliga a informar als responsables de la custodia de claus dels termes i condicions relatius a l'ús dels certificats CDS.

Així mateix, el subscriptor s'obliga a què els posseïdores de claus compleixin les seves obligacions, especificades en la fulla d'entrega corresponent.

4.5. Obligacions de custodia

El subscriptor s'obliga a custodiar, quan sigui necessari, el codi de identificació personal, la targeta o qualsevol altre suport tècnic entregat per CATCert, les claus privades i, si fos necessari, les especificacions propietat de CATCert que li siguin subministrades.

En cas de pèrdua o robatori de la clau privada del certificat CDS, o en cas de què el subscriptor sospiti que la clau privada ha perdut fiabilitat per qualsevol motiu, ha de notificar-ho immediatament a CATCert.

4.6. Obligacions d'ús correcte

El subscriptor ha d'utilitzar el servei de certificació digital, les claus pública i privada, la targeta o qualsevol altre suport tècnic entregat per CATCert, exclusivament per als usos autoritzats en la DPC, de conformitat amb el "Conveni de col·laboració", així com amb qualsevol altre instrucció, manual o procediment subministrat al subscriptor.

El subscriptor reconeixerà que quan utilitzi el certificat CDS, i mentre aquest no hagi expirat ni hagi estat suspès o revocat, s'haurà acceptat el certificat i estarà operatiu.

4.7. Transaccions prohibides

El subscriptor s'obliga a no utilitzar les seves claus privades, els certificats, les targetes o qualsevol altre suport tècnic entregat per CATCert en la realització de transacció alguna prohibida per la llei aplicable.

Els serveis de certificació digital de CATCert no han estat dissenyats ni permeten la seva 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 pogués directament causar la mort, danys físics o danys mediambientals greus.

Els certificats CDS són emesos als subscriptors per als usos expressament recollits a l'apartat primer de la clàusula segona del present Text de Divulgació.

Qualsevol altre ús fora dels descrits en la present clàusula queda expressament exclòs i formalment prohibit.

5. OBLIGACIONS DEL VERIFICADOR

5.1. Decisió informada

CATCert informa al Verificador que té accés a informació suficient per a prendre una decisió informada en el moment de verificar un Certificat CDS i confiar en la informació continguda en aquest.

El Verificador reconeix que l'ús del Registro 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.

5.2. Requisits de verificació de la signatura electrònica

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 documento electrònic signat, a fi de determinar que va ser generada per l'entitat de Certificació legítima, que és l'Agència Catalana de Certificació, utilitzant la clau privada corresponent a la clau pública continguda en el certificat del subscriptor, i que el documento no va ser modificat des de la generació de la signatura electrònica.

La comprovació del Certificat CDS serà executada normalment de forma automàtica pel software del Verificador en base als serveis i, en tot caso, de conformitat amb la DPC i amb els requisits següents:

- Utilitzar el software apropiat per a la verificació de la signatura digital del Certificat CDS amb els algoritmes 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.
- 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 de utilitzar la cadena més adequada per a verificar-la.

- Comprovar l'estat de revocació dels certificats de la cadena amb la informació subministrada en el Registro de CATCert (amb LRCs, per exemple) 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.
- 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 què 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.
- Verificar tècnicament la signatura de tots els certificats de la cadena abans de confiar en el certificat utilitzat pel signatari.
- Determinar la data i hora de generació de la signatura electrònica, ja que la signatura electrònica només pot considerar-se correctament verificada si va ser creada dins del període de vigència de la cadena de certificats en què es basa.
- Delimitar les dades que han estat signades digitalment, ja que aquestes s'utilitzaran en la verificació de la signatura.
- Verificar tècnicament la pròpia signatura amb el certificat del signatari avalat per la cadena de certificats.

5.3. Diligència exigible

El Verificador té que actuar amb la màxima diligència abans de confiar en els Certificats CDS. En concreto, el Verificador s'obliga a utilitzar el software de verificació de signatura electrònica amb la capacitat tècnica, operativa i de seguretat suficient per a executar el procés de verificació de signatura correctament, i romandrà responsable exclusiu del dany que pugui sofrir per la incorrecta elecció del mencionat software.

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

El Verificador pot confiar en un Certificat CDS si concorren les condicions següents:

- La signatura electrònica s'ha de poder verificar d'acord amb els requisits establerts en l'apartat segon de la clàusula cinquena.
- El Verificador ha d'haver utilitzat informació de revocació actualitzada en el moment de verificació de la signatura.
- El tipus i classe de Certificat CDS té que ser apropiat per al ús que es pretén fer.
- El Verificador ha de tenir en compte altres limitacions addicionals d'ús del Certificat CDS indicades de qualsevol forma en el certificat, incloent aquelles no processades automàticament pel software 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 l'apartat primer de la clàusula segona del present Text de Divulgació o altra indicació expressa de CATCert o del propi subscriptor.

- Finalment, la confiança té que ser raonable d'acord amb les circumstancies. Si les circumstancies requereixen garanties addicionals, el Verificador haurà d'obtenir aquestes garanties per a què la confiança sigui raonable.

En qualsevol cas, la decisió final amb respecto a confiar o no en un Certificat CDS 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 haurà de confiar en el Certificat CDS.

5.4. Confiança en una signatura no verificada

Queda prohibit confiar o, de qualsevol altra manera, fer ús d'una signatura o Certificat CDS no verificats.

Si el Verificador confia en un Certificat CDS, 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, de conformitat amb les Condicions d'ús, el Verificador pot confiar en les dades del certificat i/o en la signatura basada en aquest, dins de les limitacions d'ús corresponents.

5.6. Ús correcte i activitats prohibides

El Verificador s'obliga a no utilitzar cap tipus de 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.

Addicionalment, 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.

6. GARANTIES LIMITADES I REBUIG DE GARANTIES

6.1. Garantia de CATCert pels serveis de certificació digital

CATCert s'obliga a la prestació dels serveis de certificació digital en determinades condicions tècniques i operatives, tal com s'estableix en la DPC de CATCert, incloent un Registro de certificats, on es publica informació relativa a l'estat dels certificats CDS.

CATCert s'obliga a emetre informació d'estat, incloent la suspensió i la revocació, dels certificats emesos, d'acord amb la DPC.

CATCert garanteix les condicions del servei de informació següents:

- El certificat CDS conté informació correcta i actual en el moment de la seva emissió, degudament comprovada, de conformitat amb el que estableix la Llei 59/2003, de 19 de desembre.
- El certificat CDS compleix tots els requisits relatius al contingut i al format establert en la DPC.
- La clau privada de CATCert no ha estat compromesa, excepte notificació en contra mitjançant el Registro.

6.2. Exclusió de la garantia

CATCert no garanteix software algun utilitzat per qualsevol persona per a generar, verificar o utilitzar de manera distinta, cap signatura digital o certificat digital emès per CATCert, excepte quan hagi una declaració escrita en sentit contrari.

7. ACORDS APLICABLES, DPC I PDC

7.1. Acords aplicables

Els acords aplicables al certificat CDS, es contenen en el "Conveni de col·laboració de serveis de certificació", així com en les "Condicions Generals d'ús".

7.2. Declaració de Pràctiques de Certificació (DPC)

Els serveis de certificació de CATCert es regulen tècnica i operativament per la Declaració de Pràctiques de Certificació, per les seves actualitzacions posteriors, així com per documentació complementaria.

La DPC i la documentació d'operacions es modifiquen periòdicament en el Registro i es poden consultar en la pàgina de Internet http://www.catcert.net/registre.

En tot allò no previst en el present Text de Divulgació, regirà el que disposa la Declaració de Pràctiques de Certificació. Així mateix, en cas de contradicció entre els termes del present Text de Divulgació i la Declaració de Pràctiques de Certificació de CATCert, prevaldrà, en tot cas, aquesta última.

7.3. Política de Certificació (PdC)

CATCert disposa d'una política de certificació que detalla els requisits de caràcter tècnic, jurídic, operatiu, així com de regulació del Certificat CDS, a disposició de la comunitat d'usuaris que la sol·liciten.

Qualsevol divergència que es derivi d'entre el present Text de Divulgació i la Política de Certificació de CATCert, es resoldrà a favor d'aquesta última.

En tot allò no previst en el present Text de Divulgació, regirà el que disposa la Política de Certificació de CATCert. Així mateix, en cas de contradicció entre els termes del present Text de Divulgació i la Política de Certificació de CATCert, prevaldrà, en tot cas, la Política de Certificació de CATCert degudament publicada.

8. POLÍTICA DE INTIMITAT

CATCert no pot divulgar ni pot ser obligada a divulgar cap informació confidencial referent a certificats CDS sense una sol·licitud específica prèvia que provingui de:

a) la persona amb respecte a la qual CATCert té el deure de mantenir la informació confidencial, o

b) una ordre judicial, administrativa o qualsevol altra prevista en la legislació vigent.

Tot i així, el subscriptor accepta que determinada informació, personal i d'altre tipus, proporcionada en la sol·licitud de certificats, serà inclosa en els seus certificats i en el mecanisme de comprovació de l'estat dels certificats, i que la informació mencionada no té caràcter confidencial, per imperatiu legal.

CATCert no es fa responsable de l'ús que, d'aquestes dades personals, pugui fer un tercer.

9. POLÍTICA DE REINTEGRAMENT

No aplicable

10. LLEI APLICABLE I JURISDICCIÓ COMPETENT

Les parts es regiran per les lleis espanyoles, especialment per la Llei 59/2003, de 19 de desembre, de signatura electrònica, per la legislació administrativa aplicable i, subsidiàriament per la legislació civil i mercantil que regula el règim de les obligacions i els contractes.

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

11. ACREDITACIONS I SEGELLS DE QUALITAT

CATCert ha superat les auditories següents:

- WebTrust per a Autoritats de Certificació.
- Auditoria de compliment de l'especificació tècnica ETSI TS 101456.