



**Agència Catalana
de Certificació**

Text de divulgació del certificat CPISR-2

Entitat de Certificació del Parlament de Catalunya

Referència: EC-Parlament_TD_003
Versió: 1.0
Data: 14/05/2004

Informació general

Control documental

Projecte:	EC-Parlament
Entitat de destinació:	CATCert
Títol:	Text de divulgació del certificat CPISR-2
Codi de referència:	EC-Parlament_TD_003
Versió:	1.0
Data:	14/05/2004
Fitxer:	D1111_E0650_N-TD EC-Parlament CPISR-2 v1r0 cat.doc
Eina/es d'edició:	Word 2002
Autor/s:	ASTREA
Resum:	

Drets d'ús

La present documentació és propietat de l'AGÈNCIA CATALANA DE CERTIFICACIÓ, és confidencial i no podrà ésser objecte de reproducció total o parcial, tractament informàtic ni transmissió de cap forma o per qualsevol mitjà, ja sigui electrònic, mecànic, per fotocòpia, registre o qualsevol altre. Tanmateix, tampoc no podrà ésser objecte de préstec, lloguer o qualsevol forma de cessió d'ús sense el consentiment previ i per escrit de l'AGÈNCIA CATALANA DE CERTIFICACIÓ, titular del dret d'autor (copyright). L'incompliment de les limitacions assenyalades per qualsevol persona que tingui accés a la documentació serà perseguida d'acord amb la llei.

Estat formal

Preparat per:	Revisat per:	Aprovat per:
Nom: ASTREA Data: 14/05/2004	Nom: Data:	Nom: Data:

Control de versions

Versió	Parts que canvien	Descripció del canvi	Data
1.0	Tot el document	Creació del document	14/05/2004

Índex

<i>Text de divulgació del certificat CPISR-2</i>	1
Entitat de Certificació del Parlament de Catalunya.....	1
<i>Informació general</i>	2
Control documental.....	2
Drets d'ús.....	2
Estat formal.....	2
Control de versions.....	3
<i>Índex</i>	4
<u>1. INFORMACIÓ DE CONTACTE</u>	<u>6</u>
<u>1.1. Organització responsable</u>	<u>6</u>
<u>1.2. Persona de contacte</u>	<u>6</u>
<u>2. TIPUS I FINALITAT DEL CERTIFICAT CPISR-2</u>	<u>6</u>
<u>2.1. Certificat personal d'identificació i signatura reconeguda de classe 2</u>	<u>6</u>
<u>2.2. Entitat de Certificació emissora</u>	<u>7</u>
<u>3. LÍMITS D'ÚS</u>	<u>7</u>
<u>3.1. Límits d'ús adreçats als subscriptors</u>	<u>7</u>
<u>3.2. Límits d'ús adreçats als verificadors</u>	<u>8</u>
<u>4. OBLIGACIONS DELS SUBSCRIPTORS</u>	<u>8</u>
<u>4.1. Generació de claus</u>	<u>8</u>
<u>4.2. Sol·licitud de certificats</u>	<u>8</u>
<u>4.3. Veracitat de la informació</u>	<u>9</u>
<u>4.4. Lliurament i acceptació del servei</u>	<u>9</u>
<u>4.5. Obligacions de custòdia</u>	<u>9</u>
<u>4.6. Obligacions d'ús correcte</u>	<u>9</u>
<u>4.7. Transaccions prohibides</u>	<u>10</u>
<u>5. OBLIGACIONS DEL VERIFICADOR</u>	<u>10</u>
<u>5.1. Decisió informada</u>	<u>10</u>
<u>5.2. Requeriments de verificació de la signatura electrònica</u>	<u>10</u>
<u>5.3. Diligència exigible</u>	<u>12</u>

<u>5.4. Confiança en una signatura no verificada.....</u>	<u>12</u>
<u>5.5. Efecte de la verificació</u>	<u>13</u>
<u>5.6. Ús correcte i activitats prohibides.....</u>	<u>13</u>
<u>6. GARANTIES LIMITADES I REBUIG DE GARANTIES.....</u>	<u>14</u>
<u>6.1. Garantia de l'EC-Parlament pels serveis de certificació digital.....</u>	<u>14</u>
<u>6.2. Exclusió de la garantia</u>	<u>14</u>
<u>7. ACORDS APLICABLES, DPC.....</u>	<u>14</u>
<u>7.1. Acords aplicables.....</u>	<u>14</u>
<u>7.2. Declaració de pràctiques de certificació.....</u>	<u>14</u>
<u>7.3. Política de certificació.....</u>	<u>15</u>
<u>8. POLITICA D'INTIMITAT.....</u>	<u>16</u>
<u>9. POLITICA DE REINTEGRAMENT.....</u>	<u>16</u>
<u>10. LLEI APLICABLE , JURISDICCIO COMPETENT.....</u>	<u>16</u>
<u>11. ACREDITACIONS, SEGELLS DE QUALITAT.....</u>	<u>16</u>

1. INFORMACIÓ DE CONTACTE

1.1. Organització responsable

L'Entitat de Certificació del Parlament de Catalunya (EC-Parlament) és una iniciativa conjunta de:

Parlament de Catalunya

Parc de la Ciutadella, s/n

08003 – Barcelona

CATCert – Agència Catalana de Certificació

Passatge de la Concepció, 11

08008 – Barcelona

1.2. Persona de contacte

Per a qualsevol consulta, dirigiu-vos a:

Parlament de Catalunya

Parc de la Ciutadella, s/n

08003 – Barcelona

2. TIPUS I FINALITAT DEL CERTIFICAT CPISR-2

2.1. Certificat personal d'identificació i signatura reconeguda de classe 2

Els certificats personals d'identificació i signatura reconeguda de classe 2 (CPISR-2) són certificats reconeguts d'acord amb el que s'estableix a l'article 11.1, amb el contingut prescrit per l'article 11.2 i emesos a persones físiques individuals, complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

Els CPISR-2 són certificats reconeguts que funcionen amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19

de desembre, i que donen compliment a allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Per aquest motiu, els CPISR-2 garanteixen la identitat del subscriptor i la possessió de la clau privada d'identificació i signatura, i permeten la generació de la "signatura electrònica reconeguda"; és a dir, la signatura electrònica avançada que es basa en un certificat reconegut i que ha estat generada emprant un dispositiu segur, per la qual cosa, d'acord amb el que estableix l'article 3 de la Llei 59/2003, de 19 de desembre, s'equipara a la signatura escrita per efecte legal, sense necessitat de complir cap altre requeriment addicional.

Per altra banda, els CPISR-2 es poden utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura escrita, sinó només la identificació del subscriptor, com les aplicacions que s'indiquen a continuació:

- a) Autenticació en sistemes de control d'accés.
- b) Signatura de correu electrònic segur.
- c) Altres aplicacions de signatura digital.

La signatura electrònica generada en l'ús d'aquestes aplicacions tindrà els efectes que en determini la normativa reguladora de l'aplicació, que podrà declarar l'equivalència amb la signatura escrita o només l'efecte d'identificació, ja que, si més no, aquesta signatura haurà estat produïda amb el dispositiu segur.

Els CPISR-2 s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.82.

2.2. Entitat de Certificació emissora

Els CPISR-2 són emesos per l'Entitat de Certificació del Parlament de Catalunya (EC-Parlament), operada per CATCert sota la direcció del Parlament.

CATCert és el prestador de serveis de certificació que emet els certificats de l'EC-Parlament, seguint les seves indicacions.

El Parlament actua també com Entitat de Registre Col·laboradora, oferint suport a les Institucions i els usuaris de signatura electrònica.

3. LÍMITS D'ÚS

3.1. Límits d'ús adreçats als subscriptors

El subscriptor ha d'utilitzar el servei de certificació CPISR-2 prestat per l'EC-Parlament exclusivament per als usos autoritzats a les "Condicions Generals d'emissió" (vegeu Obligacions del subscriptor).

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

El subscriptor ha de complir qualsevol llei i regulació que pugui afectar el seu dret a utilitzar les eines criptogràfiques que empli.

El subscriptor no pot adoptar mesures d'inspecció, alteració o enginyeria inversa dels serveis de certificació digital de l'EC-Parlament, sense previ permís exprés.

3.2. Límits d'ús adreçats als verificadors

El verificador ha d'utilitzar el servei de certificació CPISR-2, i el corresponent servei d'informació, prestat per l'EC-Parlament, exclusivament per als usos autoritzats a les "Condicions generals d'ús del certificat CPISR-2"(vegeu Obligacions del verificador).

Així mateix, el verificador s'obliga a utilitzar el servei de certificació digital d'acord amb les instruccions, manuals o procediments subministrats per l'EC-Parlament.

El verificador reconeix que el certificat no garanteix la capacitat del subscriptor per realitzar actes concrets, perquè no inclou cap esment a l'actual capacitat general d'obrar, ni a les seves autoritzacions o poders. Per tant, l'eficàcia jurídica del document o missatge signat dependrà en tot cas de que el verificador faci les comprovacions addicionals corresponents.

El verificador ha de complir qualsevol llei i regulació que pugui afectar el seu dret a utilitzar les eines criptogràfiques que empli.

El verificador no pot adoptar mesures d'inspecció, alteració o enginyeria inversa dels serveis de certificació digital de l'EC-Parlament, sense previ permís exprés.

4. OBLIGACIONS DELS SUBSCRIPTORS

4.1. Generació de claus

El subscriptor ha de generar les seves pròpies claus, privada i pública, per a la identificació i la signatura electrònica dins un dispositiu segur de creació de signatura electrònica (la targeta que rep el posseïdor de claus), i sol·licita l'emissió del certificat CPISR-2.

4.2. Sol·licitud de certificats

El subscriptor s'obliga a realitzar les sol·licituds de certificats de classe 2 d'acord amb el procediment i, si s'escau, els components tècnics subministrats per l'EC-Parlament, d'acord amb el que s'estableix a la DPC i a la documentació d'operacions de l'EC-Parlament.

4.3. Veracitat de la informació

El subscriptor es responsabilitza que tota la informació inclosa a la seva sol·licitud del certificat sigui exacta, completa per a la finalitat del certificat i estigui actualitzada en tot moment.

El subscriptor ha d'informar immediatament a l'EC-Parlament de qualsevol inexactitud en el certificat detectada un cop s'hagi emès, així com dels canvis que es produeixin en la informació aportada i/o registrada per la Institució per a l'emissió del certificat.

4.4. Lliurament i acceptació del servei

Amb la signatura del full de lliurament, el subscriptor reconeix que s'ha lliurat la targeta, el certificat, la clau privada i qualsevol altre suport tècnic lliurat per l'EC-Parlament, així com, quan pertoqui, el codi d'identificació personal, i que aquests elements funcionen correctament.

El subscriptor accepta, amb la signatura del full de lliurament o mitjançant el procediment telemàtic d'acceptació de certificats, el certificat, segons s'especifica a la DPC de l'EC-Parlament.

4.5. Obligacions de custòdia

El subscriptor s'obliga a custodiar, quan s'escaigui, el codi d'identificació personal, la targeta o qualsevol altre suport tècnic lliurat per l'EC-Parlament, les claus privades i, si s'escau, les especificacions propietat de l'EC-Parlament que li siguin subministrades, així com tota la informació que generi

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

4.6. Obligacions d'ús correcte

El subscriptor ha d'utilitzar el servei de certificació CPISR-2 prestat per l'EC-Parlament, exclusivament per als usos autoritzats a la DPC i qualsevol altra instrucció, manual o procediment subministrats al subscriptor.

El subscriptor ha de complir qualsevol llei i regulació que pugui afectar el seu dret a utilitzar les eines criptogràfiques que empri.

El subscriptor no podrà adoptar mesures d'inspecció, alteració o enginyeria inversa dels serveis de certificació digital de classe 2 prestats.

El subscriptor reconeixerà:

-
- a) Que totes les comunicacions electròniques, degudament autoritzades, autenticades amb la signatura digital generada amb la clau privada del posseïdor de claus de certificats CPISR-2 tenen el mateix efecte legal, validesa i força vinculant que una comunicació escrita i degudament autenticada.
- b) Que quan utilitzi qualsevol certificat, i mentre el certificat no hagi expirat ni hagi estat suspès o revocat, s'haurà acceptat el certificat i estarà operatiu.
- c) Que no actua com a entitat de certificació i, per tant, s'obliga a no utilitzar les claus privades corresponents a les claus públiques contingudes en els certificats amb el propòsit de signar cap certificat.

4.7. Transaccions prohibides

El subscriptor s'ha d'obligar a no utilitzar les seves claus privades, els certificats, les targetes o qualsevol altre suport tècnic lliurat per l'EC-UR per realitzar cap transacció prohibida per la llei aplicable.

Els serveis de certificació digital prestats per l'EC-Parlament no han estat dissenyats ni permeten la seva utilització o revenda com a equips de control de situacions perilloses, o per a usos que requereixin actuacions a prova d'errors, com ara l'operació d'instal·lacions nuclears, sistemes de navegació o comunicació aèria, sistemes de control de trànsit aeri o sistemes de control d'armament, on una errada pogués directament causar la mort, danys físics o danys mediambientals greus.

5. OBLIGACIONS DEL VERIFICADOR

5.1. Decisió informada

L'EC-Parlament informa al verificador que té accés a informació suficient per prendre una decisió informada en el moment de verificar un certificat i confiar en la informació continguda al certificat.

Addicionalment, el verificador reconeixerà que l'ús del Registre i de les Llistes de Revocació de Certificats (en endavant, "les LRCs" o "les "CRLs") de l'EC-Parlament, es regeix per la DPC de l'EC-Parlament i es comprometrà a complir els requeriments tècnics, operatius i de seguretat descrits a l'esmentada DPC.

5.2. Requeriments de verificació de la signatura electrònica

Per confiar en un missatge o document, el verificador ha de validar dues signatures:

- En primer lloc, ha de verificar la signatura electrònica del missatge o document. Aquesta comprovació és imprescindible per determinar que va ésser generada

pel subscriptor, utilitzant la clau privada corresponent a la clau pública continguda al certificat CPISR-2, i per garantir que el missatge o document signat no va ésser modificat des de la generació de la signatura electrònica.

- En segon lloc, ha de verificar la signatura electrònica del certificat CPISR-2 del subscriptor. Aquesta comprovació és imprescindible per determinar que la clau pública continguda al certificat correspon al subscriptor, i per tant, la seva identitat, i legitimitació per signar.

La comprovació serà executada normalment de forma automàtica pel programari del verificador i, en tot cas, d'acord amb la DPC, amb els següents requeriments:

- Cal utilitzar el programari apropiat per a la verificació d'una signatura digital amb els algorismes i longituds de claus autoritzats al certificat i/o executar qualsevol altra operació criptogràfica, i establir la cadena de certificats en què es basa la signatura electrònica a verificar, ja què la signatura electrònica es verifica utilitzant aquesta cadena de certificats.
- Cal assegurar que la cadena de certificats identificada és la més adequada per a la signatura electrònica que es verifica, ja què 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 adient per verificar-la.
- Cal comprovar l'estat de revocació dels certificats de la cadena amb la informació subministrada al Registre de l'EC-Parlament (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 cadascun dels certificats de la cadena són correctes i es troben vigents.
- Cal 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 incloguin 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.
- Cal verificar tècnicament la signatura de tots els certificats de la cadena abans de confiar en el certificat utilitzat pel signatari.
- Cal determinar la data i hora de generació de la signatura electrònica, ja què la signatura electrònica només pot considerar-se correctament verificada si va ésser creada dins el període de vigència de la cadena de certificats en què es basa.
- Cal delimitar les dades que han estat signades digitalment, ja què les mateixes s'utilitzaran a la verificació de la signatura.
- Finalment, cal 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 els certificats i les signatures digitals. En concret, el verificador s'obliga a utilitzar 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 romandrà responsable exclusiu del dany que pugui patir per la incorrecta elecció de l'esmentat programari.

La prescripció anterior no serà aplicable quan l'EC-Parlament hagi subministrat el programari de verificació al verificador.

El verificador pot confiar en un missatge o document signat si concorren les següents condicions:

- La signatura electrònica s'ha de poder verificar d'acord amb els requeriments establerts a l'apartat 5.2.
- El verificador ha d'haver utilitzat informació de revocació actualitzada en el moment de verificació de la signatura
- El tipus i classe de certificat ha d'ésser apropiat per a l'ús que se'n pretén fer
- El verificador ha de prendre en consideració altres limitacions addicionals d'ús del certificat indicades de qualsevol manera al certificat, incloent-hi 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 l'EC-Parlament al subscriptor o al posseïdor de claus, més enllà de la descripció del certificat segons l'apartat 2 anterior o una altra indicació expressa de l'EC-Parlament o del propi subscriptor.
- El verificador ha d'establir el significat de la signatura i la intenció del signatari, doncs l'acte de signar pot tenir implicacions diferents segons l'aplicació de la signatura, com protegir una transmissió o prestar el consentiment.
- Finalment, la confiança ha d'ésser raonable d'acord amb les circumstàncies. Si les circumstàncies requereixen garanties addicionals, el verificador haurà d'obtenir aquestes garanties per a què la confiança sigui raonable.

En qualsevol cas, la decisió final respecte a confiar o no en una signatura electrònica verificada és exclusivament del verificador.

5.4. Confiança en una signatura no verificada

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

Si el verificador confia en una signatura electrònica no verificada, assumirà tots els riscos derivats d'aquesta actuació.

5.5. Efecte de la verificació

En virtut de la correcta verificació d'una signatura i els certificats, d'acord amb les condicions generals d'ús, el verificador pot confiar en la identificació i, en el seu cas, signatura del subscriptor o posseïdor de claus, dins de les limitacions d'ús corresponents.

El verificador reconeix i accepta que, allà on es requereixi que una transacció sigui realitzada per escrit, un missatge o document que contingui una signatura digital verificable utilitzant el certificat és tan vàlid i efectiu com si hagués estat realitzat per escrit i signat en paper.

Així mateix, sempre conforme amb la llei aplicable, la signatura o la transacció digital serà efectiva amb independència de la localització geogràfica d'emissió de la mateixa o de la creació o ús de la signatura digital, així com de la localització de l'EC-Parlament, del subscriptor o del posseïdor de claus.

5.6. Ús correcte i activitats prohibides

El verificador s'obliga a no utilitzar cap mena d'informació d'estat dels certificats o de cap altre tipus que hagi estat subministrada per l'EC-Parlament, per realitzar cap transacció prohibida per la llei aplicable a la citada transacció.

El verificador s'obliga a no inspeccionar, interferir o realitzar enginyeria inversa a la implantació tècnica dels serveis públics de certificació de l'EC-Parlament, sense previ consentiment escrit.

Adicionalment, el verificador s'obliga a no comprometre intencionadament la seguretat dels serveis públics de certificació de l'EC-Parlament.

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

6. GARANTIES LIMITADES I REBUIG DE GARANTIES

6.1. Garantia de l'EC-Parlament pels serveis de certificació digital

L'EC-Parlament garanteix que la clau privada de l'entitat de certificació utilitzada per emetre certificats no ha estat compromesa, llevat que l'EC-Parlament no hagi comunicat el contrari mitjançant el Registre de certificació, d'acord amb la DPC.

L'EC-Parlament també garanteix que:

- a) Els certificats contenen tota la informació exigida per la Llei 59/2003, de 19 de desembre.
- b) No ha originat ni ha introduït declaracions falses o errònies a la informació de cap certificat, ni ha deixat d'incloure informació necessària aportada pel subscriptor i validada per l'EC-Parlament, en el moment de l'emissió del certificat.
- c) Tots els certificats compleixen els requeriments formals i de contingut de la DPC.
- d) Queda vinculada pels procediments operatius i de seguretat descrits a la DPC.

6.2. Exclusió de la garantia

L'EC-Parlament no garanteix cap programari que utilitzi qualsevol persona per generar, verificar o utilitzar d'una altra forma cap signatura digital o certificat digital emès per l'EC-Parlament, excepte que hi hagi una declaració escrita en sentit contrari.

7. ACORDS APLICABLES, DPC.

7.1. Acords aplicables

Els acords aplicables al certificat CPISR-2, vénen continguts en les Condicions Generals d'Emissió, així com en les condicions Generals d'Ús.

7.2. Declaració de pràctiques de certificació

Els serveis de certificació de l'EC-Parlament es regulen tècnicament i operativament per la Declaració de pràctiques de certificació per les seves actualitzacions posteriors, així com per documentació complementària.

La DPC i la documentació d'operacions es modifica periòdicament al Registre i és consultable a la pàgina [\[proposar adreça\]](#).

7.3. Política de certificació

L EC-Parlament disposa d'una política de certificació que detalla els requisits de caràcter tècnic, jurídic, operatiu, així com de regulació del certificat CPISR-2, a disposició de la comunitat d usuaris que la sol·licitin.

8. POLITICA D'INTIMITAT

L'EC-Parlament no pot divulgar ni pot ésser obligada a divulgar cap informació confidencial referent a certificats sense una sol·licitud específica prèvia que provingui de:

- a) la persona respecte a la qual l'EC-Parlament té el deure de mantenir la informació confidencial, o
- b) una ordre judicial, administrativa o qualsevol altra prevista en la legislació vigent.

Tot i això, el subscriptor accepta que determinada informació, personal i d'altre tipus, proporcionada a la sol·licitud de certificats, serà inclosa als seus certificats i al mecanisme de comprovació de l'estat dels certificats, i que la informació esmentada no tindrà caràcter confidencial, per imperatiu legal.

9. POLITICA DE REINTEGRAMENT

Donat el caràcter gratuït del certificat de CPISR-2 per a les persones físiques que el reben i l'utilitzen, no es preveu l'esmentada política.

10. LLEI APLICABLE , JURISDICCIO COMPETENT

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

La jurisdicció competent serà la jurisdicció civil, d'acord amb les normes contingudes a la Llei 1/2000, de 7 de gener.

11. ACREDITACIONS, SEGELLS DE QUALITAT

No aplicable.