



**Agència Catalana
de Certificació**

Text de divulgació del CPISR-1 Càrrec
Entitat de Certificació d'Universitats i Recerca

Referència: D1111_E0650_N – TD CPISR-1 Càrrec EC-UR
Versió: 1.0
Data: 31/01/2005

Índex

Entitat de Certificació d'Universitats i Recerca.....	1
<i>Índex</i>	2
<u>1. INFORMACIÓ DE CONTACTE</u>	<u>4</u>
<u>1.1. Organització responsable</u>	<u>4</u>
<u>1.2. Persona de contacte</u>	<u>4</u>
<u>2. TIPUS I FINALITAT DEL CERTIFICAT CPISR-1 CÀRREC</u>	<u>4</u>
<u>3. LÍMITS D'ÚS</u>	<u>6</u>
<u>3.1. Límits d'ús adreçats als subscriptors</u>	<u>6</u>
<u>3.2. Límits d'ús adreçats als verificadors</u>	<u>6</u>
<u>4. OBLIGACIONS DELS SUBSCRIPTORS</u>	<u>7</u>
<u>4.1. Generació de claus</u>	<u>7</u>
<u>4.2. Sol·licitud de certificats</u>	<u>7</u>
<u>4.3. Veracitat de la informació</u>	<u>7</u>
<u>4.4. Obligacions com a entitat de registre</u>	<u>7</u>
<u>4.5. Nomenament d'operadors d'entitat de registre</u>	<u>8</u>
<u>4.6. Diligència exigible</u>	<u>8</u>
<u>4.7. Delegació de les funcions d'entitats de registre</u>	<u>9</u>
<u>4.8. Lliurament i acceptació del servei</u>	<u>9</u>
<u>4.9. Possedors de claus de la Institució</u>	<u>9</u>
<u>4.10. Obligacions de custòdia</u>	<u>9</u>
<u>4.11. Obligacions d'ús correcte</u>	<u>10</u>
<u>4.12. Transaccions prohibides</u>	<u>10</u>
<u>5. OBLIGACIONS DEL VERIFICADOR</u>	<u>11</u>
<u>5.1. Decisió informada</u>	<u>11</u>
<u>5.2. Requeriments de verificació de la signatura electrònica</u>	<u>11</u>
<u>5.3. Diligència exigible</u>	<u>12</u>
<u>5.4. Confiança en una signatura no verificada</u>	<u>13</u>
<u>5.5. Efecte de la verificació</u>	<u>13</u>
<u>5.6. Ús correcte i activitats prohibides</u>	<u>14</u>

<u>6. GARANTIES LIMITADES I REBUIG DE GARANTIES.....</u>	<u>14</u>
<u>6.1. Garantia de CATCert pels serveis de certificació digital.....</u>	<u>14</u>
<u>6.2. Exclusió de la garantia</u>	<u>15</u>
<u>7. ACORDS APLICABLES, DPC.....</u>	<u>15</u>
<u>7.1. Acords aplicables.....</u>	<u>15</u>
<u>7.2. Declaració de pràctiques de certificació.....</u>	<u>15</u>
<u>7.3. Política de certificació.....</u>	<u>15</u>
<u>8. POLÍTICA D'INTIMITAT.....</u>	<u>15</u>
<u>9. POLÍTICA DE REINTEGRAMENT.....</u>	<u>16</u>
<u>10. LLEI APLICABLE , JURISDICCió COMPETENT.....</u>	<u>16</u>
<u>11. ACREDITACIONS, SEGELLS DE QUALITAT.....</u>	<u>16</u>

1. INFORMACIÓ DE CONTACTE

1.1. Organització responsable

Centre de Supercomputació de Catalunya (CESCA)

Gran Capità, 2-4

(Edifici Nexus)

08034 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:

Centre de Supercomputació de Catalunya (CESCA)

Gran Capità, 2-4

(Edifici Nexus)

08034 Barcelona

CATCert – Agència Catalana de Certificació

Àrea d'assessorament i recerca

Passatge de la Concepció, 11

08008 – Barcelona

2. TIPUS I FINALITAT DEL CERTIFICAT CPISR-1 CÀRREC

Els certificats personals d'identificació i signatura reconeguda (en endavant, CPISR-1 Càrrec) 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 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-1 Càrrec 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-1 Càrrec garanteixen la identitat del subscriptor i del posseïdor 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.

Els certificats CPISR-1 Càrrec inclouen una manifestació relativa a la categoria de personal i càrrec del posseïdor de claus, que han estat comprovats abans d'emetre el certificat, i són correctes. Tot i això, aquesta indicació no és, per si sola, suficient per determinar les facultats que té el posseïdor de claus per signar en nom del subscriptor; per tant, l'usuari del certificat haurà de comprovar les facultats i poders de signatura del posseïdor mitjançant altres mitjans, diferents al certificat.

Per altra banda, els CPISR-1 es poden utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura escrita, sinó només la identificació del posseïdor de claus, en nom de la Institució, 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-1 Càrrec són certificats per a personal de la Institució, dins del seu àmbit corporatiu, i no emesos per al públic. Aquest personal té la consideració de posseïdor de claus i de la targeta i el programari complementari corresponents.

Els CPISR-1 càrrec emesos per l'EC-UR s'identifiquen amb l'identificador de l'objecte (OID):

OID: 1.3.6.1.4.1.15096.1.3.1.81.2

3. LÍMITS D'ÚS

3.1. Límits d'ús adreçats als subscriptors

El subscriptor ha d'utilitzar el servei de certificació CPISR-1 Càrrec prestat per CATCert exclusivament per als usos autoritzats a la clàusula quarta, secció onzena, del Conveni de col·laboració de serveis de certificació, que es reproduïx posteriorment (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 CATCert.

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 descompilació dels serveis de certificació digital de CATCert, sense el previ permís exprés de CATCert.

3.2. Límits d'ús adreçats als verificadors

El verificador ha d'utilitzar el servei de certificació CPISR-1 Càrrec, i el corresponent servei d'informació, prestat per CESCO conjuntament amb CATCert, exclusivament per als usos autoritzats a la clàusula tercera de les Condicions generals d'ús del certificat CPISR-1 Càrrec, que es reproduïx posteriorment (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 CATCert.

El verificador reconeix que el certificat no garanteix la capacitat del subscriptor per realitzar actes concrets, perquè no inclou cap esment a la majoria d'edat, ni a la 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 descompilació dels serveis de certificació digital de CATCert, sense el previ permís exprés de CATCert.

4. OBLIGACIONS DELS SUBSCRIPTORS

4.1. Generació de claus

El subscriptor genera 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-1 càrrec.

4.2. Sol·licitud de certificats

La Institució s'obliga a realitzar les sol·licituds de certificats de classe 1 d'acord amb el procediment i, si s'escau, els components tècnics subministrats per CESCA, d'acord amb el que s'estableix a la DPC i a la documentació d'operacions de CATCert.

4.3. Veracitat de la informació

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

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

4.4. Obligacions com a entitat de registre

Amb independència de la seva condició i responsabilitat com a subscriptor de certificats de classe 1, la Institució s'obliga a complir totes les funcions d'una entitat de registre; és a dir, la validació i l'aprovació de sol·licituds de certificats i la posterior generació de targetes per als posseïdors de claus, d'acord amb els procediments i els instruments tècnics establerts per CESCA, en col·laboració amb CATCert, i d'acord amb la DPC i la documentació d'operacions de CATCert.

La Institució només pot formular i aprovar una sol·licitud de certificat si la persona és un individu vinculat a la Institució, d'acord amb el que s'estableix a la política de certificació CPISR de classe 1 amb càrrec.

Si la Institució no disposa d'informació actualitzada del posseïdor de claus, ha de comprovar-ne la identitat personalment o utilitzant sistemes que proporcionin garanties equivalents a la identificació amb presència física del futur posseïdor de claus, i enregistrar una justificació acreditativa del nom complet, lloc i data de naixement, DNI o qualsevol altra informació que pugui ésser utilitzada per diferenciar

una persona d'altres dins l'àmbit de la Institució. Es considera que la informació del posseïdor enregistrada per la Institució en els últims cinc anys està actualitzada.

La Institució ha de verificar, quan sigui aplicable, qualsevol atribut específic del posseïdor de claus, i registrar una justificació acreditativa de la informació.

La Institució ha de comprovar les dades associades al dispositiu i, si s'escau, les dades de la persona responsable del dispositiu servidor segur o editor del programari.

Així mateix, s'obliga realitzar i/o tramitar les sol·licituds de suspensió, reactivació, revocació i renovació de certificats, d'acord amb els procediments i els instruments tècnics establerts per CATCert, i d'acord amb la DPC i la documentació d'operacions de CATCert.

En el cas que un posseïdor de claus a qui s'hagi emès un certificat cessi en la seva vinculació amb la Institució, aquest ha de sol·licitar immediatament la revocació del certificat.

Adicionalment, la Institució s'obliga a emmagatzemar els registres (en paper o electrònicament, segons s'escaigui) referents a la informació continguda en el certificat durant un període de quinze anys, excepte en cas de delegació del registre al CESCA. Els registres han d'estar a disposició de CESCA i de CATCert en tot moment.

4.5. Nomenament d'operadors d'entitat de registre

Per dur a terme les obligacions anteriorment indicades per mitjans telemàtics, la Institució ha de nomenar operador de l'autoritat de registre dos o més dels seus treballadors i ha de comunicar al CESCA les dades d'aquestes persones perquè emeti els certificats CPISR-1 Càrrec corresponents.

Quan un operador deixi de tenir la capacitat d'actuar com a tal sota el control i l'autoritat de la Institució, aquest ha de sol·licitar immediatament a CATCert la revocació del seu certificat CPISR-1 Càrrec.

4.6. Diligència exigible

La Institució ha d'executar les tasques establertes en aquest annex amb la màxima diligència i ha de nomenar com operador únicament personal amb la formació i qualificació suficients.

Els operadors han de rebre de CESCA, en col·laboració amb CATCert, la formació necessària per a l'execució de les seves obligacions.

La Institució garanteix al CESCA i a CATCert que ha complert aquest conveni, la DPC vigent i la documentació d'operacions de CATCert en la seva tasca com a entitat de registre.

4.7. Delegació de les funcions d'entitats de registre

La Institució pot contractar les funcions d'entitat de registre al CESCA, d'acord amb el que s'estableix a l'annex de registre delegat.

4.8. Lliurament i acceptació del servei

Amb la signatura del full de lliurament, el subscriptor i, si s'escau, el posseïdor de claus reconeixen que se'ls ha lliurat la targeta, el certificat, la clau privada i qualsevol altre suport tècnic lliurat pel CESCA, així com, quan pertoqui, el codi d'identificació personal, i que aquests elements funcionen correctament.

El subscriptor i, si s'escau, el posseïdor de claus accepten, amb la signatura del full de lliurament, el certificat. Així mateix, el subscriptor queda vinculat pels termes de la política de certificat aplicable, segons s'especifica a la Declaració de pràctiques de certificació de CATCert.

El posseïdor accepta el certificat mitjançant el procediment telemàtic d'acceptació de certificats descrit a la DPC de CATCert.

El subscriptor ha de gestionar la signatura del full de lliurament de posseïdors de claus i l'ha de custodiar durant un període de quinze anys, excepte quan delegui el registre al CESCA.

4.9. Posseïdors de claus de la Institució-

La Institució s'obliga informar els posseïdors de claus dels termes i condicions relatius a l'ús dels certificats de classe 1.

També s'obliga que els posseïdors de claus compleixin les seves obligacions, especificades al full de lliurament corresponent.

4.10. 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 pel CESCA, les claus privades i, si s'escau, les especificacions propietat del CESCA o CATCert que li siguin subministrades, així com tota la informació que generi en la seva activitat com a entitat de registre.

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 al CESCA.

4.11. Obligacions d'ús correcte

El subscriptor ha d'utilitzar el servei de certificació de classe 1 prestat pel CESCO, en col·laboració amb CATCert, exclusivament per als usos autoritzats a la política de certificació aplicable.

El subscriptor s'obliga a utilitzar el servei de certificació digital de classe 1, la parella clau pública/clau privada, la targeta o qualsevol altre suport tècnic lliurat pel CESCO i els certificats d'acord amb aquest conveni, i qualsevol altre instrucció, manual o procediment subministrats pel CESCO al subscriptor.

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 descompilació dels serveis de certificació digital de classe 1 prestats.

El subscriptor reconeix:

- a) Que totes les comunicacions electròniques autenticades amb la signatura digital generada amb la clau privada del posseïdor de claus de certificats CPISR tenen el mateix efecte legal, vàlidesa i força vinculant que una comunicació escrita i degudament autenticada.
- b) Que la signatura digital generada amb la clau privada del posseïdor de claus de certificats CPISR és la signatura electrònica vàlida del subscriptor.
- c) 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.
- d) 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.

4.12. Transaccions prohibides

El subscriptor s'obliga a no utilitzar les seves claus privades, els certificats, les targetes o qualsevol altre suport tècnic lliurat pel CESCO per realitzar cap transacció prohibida per la llei aplicable.

Els serveis de certificació digital prestats pel CESCO, en col·laboració amb CATCert, 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

CATCert informa al verificador, que es dóna per notificat, 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.

Adicionalment, 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 requeriments tècnics, operatius i de seguretat descrits a l'esmentada DPC de CATCert.

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 o pel posseïdor de claus, utilitzant la clau privada corresponent a la clau pública continguda al certificat CPISR-1 Càrrrec, 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-1 Càrrrec del subscriptor o del posseïdor de claus. Aquesta comprovació és imprescindible per determinar que la clau pública continguda al certificat correspon al subscriptor o al posseïdor, i per tant, la seva identitat, legitimació per signar i, en el cas del posseïdor de claus, la seva vinculació amb el subscriptor.

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 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 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 CATCert 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 CATCert 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 CATCert 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 CATCert, 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 CATCert, 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 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 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 CATCert pels serveis de certificació digital

CATCert i CESCA garanteixen que la clau privada de l'entitat de certificació utilitzada per emetre certificats no ha estat compromesa, llevat que CATCert no hagi comunicat el contrari mitjançant el registre de certificació de CATCert, d'acord amb la Declaració de pràctiques de certificació.

CATCert i CESCA únicament garanteixen que:

- a) Els certificats reconeguts contenen tota la informació exigida per la Llei 59/2003, de 19 de desembre.
- b) CATCert i CESCA no han originat ni han introduït declaracions falses o errònies a la informació de cap certificat, ni ha deixat d'incloure informació necessària aportada pel subscriptor i validada per CATCert o per l'entitat de registre col·laboradora, en el moment de l'emissió del certificat.
- c) Tots els certificats compleixen els requeriments formals i de contingut de la Declaració de pràctiques de certificació del certificat CPISR-1 Càrrec.
- d) CATCert i CESCA queden vinculats pels procediments operatius i de seguretat descrits a la Declaració de pràctiques de certificació de CATCert.

6.2. Exclusió de la garantia

CATCert i CESCA no garanteixen cap programari que utilitzi qualsevol persona per generar, verificar o utilitzar d'una altra forma cap signatura digital o certificat digital emès per CATCert, excepte que hi hagi una declaració escrita de CATCert en sentit contrari.

7. ACORDS APLICABLES, DPC.

7.1. Acords aplicables

Els acords aplicables al certificat CPISR-1 Càrrrec, vénen continguts 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

Els serveis de certificació de CATCert es regulen tècnicament i operativament per la Declaració de pràctiques de certificació de CATCert (en endavant, DPC) i per les seves actualitzacions posteriors, així com per documentació complementària subministrada a la Institució.

La DPC i la documentació d'operacions de CATCert, que es modifica periòdicament al Registre i és consultable a la pàgina <http://www.catcert.net/registre>, s'incorporen a aquest conveni per referència.

7.3. Política de certificació

CATCert disposa d'una política de certificació que detalla els requisits de caràcter tècnic, jurídic, operatiu, així com de regulació del certificat CPISR-1 Càrrrec, a disposició de la comunitat d'usuaris que la sol·licitin.

8. POLÍTICA D'INTIMITAT

CATCert 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 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 això, el ciutadà 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. POLÍTICA DE REINTEGRAMENT

Donat el caràcter gratuït del certificat de CPISR-1 Càrrrec 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, així com per la legislació administrativa aplicable.

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

11.ACREDITACIONS, SEGELLS DE QUALITAT

No aplicable.