



**Agència Catalana
de Certificació**

**Text de divulgació del certificat
CEIXSA-1**

Entitat de Certificació Universitats i Recerca

Referència:
Versió: 1.0
Data: 14/07/2009

Índex

<i>Text de divulgació del certificat CEIXSA-1</i>	1
Entitat de Certificació Universitats i Recerca	1
<i>Índex</i>	2
<u>1. INFORMACIÓ DE CONTACTE</u>	4
<u>1.1. Organització responsable</u>	4
<u>1.2. Persona de contacte</u>	4
<u>2. TIPUS I FINALITAT DEL CERTIFICAT CEIXSA</u>	4
<u>2.1. Certificat d'Entitat d'Identificació, Xifrat i Signatura Avançada</u>	4
<u>2.2. Entitat de Certificació emissora</u>	5
<u>3. LÍMITS D'ÚS</u>	5
<u>3.1. Límits d'ús adreçats als subscriptors</u>	5
<u>3.2. Límits d'ús adreçats als verificadors</u>	6
<u>4. OBLIGACIONS DELS SUBSCRIPTORS</u>	6
<u>4.1. Generació de claus</u>	6
<u>4.2. Sol·licitud de certificats</u>	6
<u>4.3. Veracitat de la informació</u>	6
<u>4.4. Obligacions com a entitat de registre</u>	7
<u>4.5. Lliurament i acceptació del servei</u>	7
<u>4.6. Possedors de claus del subscriptor</u>	8
<u>4.7. Obligacions de custòdia</u>	8
<u>4.8. Obligacions d'ús correcte</u>	8
<u>4.9. Transaccions prohibides</u>	9
<u>5. OBLIGACIONS DEL VERIFICADOR</u>	9
<u>5.1. Decisió informada</u>	9
<u>5.2. Requeriments de verificació de la signatura electrònica</u>	9
<u>5.3. Diligència exigible</u>	10
<u>5.4. Confiança en una signatura no verificada</u>	11
<u>5.5. Efecte de la verificació</u>	11
<u>5.6. Ús correcte i activitats prohibides</u>	12

<i><u>6. GARANTIES LIMITADES I REBUIG DE GARANTIES.....</u></i>	<i><u>12</u></i>
6.1. Garantia de l'EC-UR pels serveis de certificació digital.....	12
6.2. Exclusió de la garantia	13
<i><u>7. ACORDS APLICABLES, DPC.....</u></i>	<i><u>13</u></i>
7.1. Acords aplicables.....	13
7.2. Declaració de pràctiques de certificació.....	13
7.3. Política de certificació.....	13
<i><u>8. POLITICA D'INTIMITAT.....</u></i>	<i><u>13</u></i>
<i><u>9. POLITICA DE REINTEGRAMENT.....</u></i>	<i><u>14</u></i>
<i><u>10. LLEI APLICABLE , JURISDICCió COMPETENT.....</u></i>	<i><u>14</u></i>
<i><u>11. ACREDITACIONS, SEGELLS DE QUALITAT.....</u></i>	<i><u>14</u></i>

1. INFORMACIÓ DE CONTACTE

1.1. Organització responsable

L'Entitat de Certificació Universitats i Recerca, en endavant EC-UR, és una iniciativa de:

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)

Servei de Certificació Digital

Gran Capità, 2-4

(Edifici Nexus)

08034 Barcelona

2. TIPUS I FINALITAT DEL CERTIFICAT CEIXSA

2.1. Certificat d'Entitat d'Identificació, Xifrat i Signatura Avançada

Els certificats d'entitat d'identificació, xifrat i signatura electrònica avançada són certificats reconeguts, no emesos al públic, d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emesos complint les obligacions dels articles 7, 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura

electrònica, i que donen compliment al dispostat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

S'utilitzen per a signar missatges d'autenticació (confirmació de la identitat) i d'accés segur a sistemes informàtics, per a rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, utilitzant la clau pública del subscriptor indicada en el CEIXSA i per a signatura documents sense dispositiu segur de creació de signatura, donant suport a la signatura electrònica avançada segons l'article 3.2 de la Llei 59/2003, de 19 de desembre.

Els CEIXSA garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten la generació de la "signatura electrònica avançada", d'acord amb el que estableix l'article 3 de la Llei 59/2003, de 19 de desembre, sense perjudici de que una norma que reguli un determinat procediment estableixi l'equivalència amb la signatura manuscrita.

Els CEIXSA són certificats per la Institució, i no emesos per al públic. El personal de la Institució que rep el certificat té la consideració de posseïdor i responsable de custòdia de les claus, així com de la targeta i el programari complementari corresponents.

Els CEIXSA emesos per l'EC-UR s'identifiquen amb l'identificador de l'objecte (OID):
Classe 1: 1.3.6.1.4.1.15096.1.3.1.161.3

2.2. Entitat de Certificació emissora

Els CEIXSA són emesos per l'Entitat Universitats i Recerca, operada per CATCert. CATCert és el prestador de serveis de certificació que emet els certificats de l'EC-UR, seguint les seves indicacions.

3. LÍMITS D'ÚS

3.1. Límits d'ús adreçats als subscriptors

El subscriptor ha d'utilitzar el servei de certificació CEIXSA prestat per l'EC-UR exclusivament per als usos autoritzats al "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 l'EC-UR.

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 pot adoptar mesures d'inspecció, alteració o enginyeria inversa dels serveis de certificació digital de l'EC-UR, sense previ permís exprés.

3.2. Límits d'ús adreçats als verificadors

El verificador ha d'utilitzar el servei de certificació CEIXSA, i el corresponent servei d'informació, prestat per l'EC-UR, exclusivament per als usos autoritzats a les "Condicions generals d'ús del certificat CEIXSA", 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 l'EC-UR.

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

El verificador no pot adoptar mesures d'inspecció, alteració o enginyeria inversa dels serveis de certificació digital de l'EC-UR, 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 CEIXSA .

4.2. Sol·licitud de certificats

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

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-UR 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

El subscriptor 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 l'EC-UR, i d'acord amb la DPC i la documentació d'operacions de l'EC-UR.

El subscriptor només pot formular i aprovar una sol·licitud de certificat si la persona és un individu vinculat al subscriptor. Si el subscriptor 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, document nacional d'identitat o equivalent, o qualsevol altra informació que pugui ésser utilitzada per diferenciar una persona d'altres dins l'àmbit del subscriptor.

El subscriptor ha de verificar, quan sigui aplicable, qualsevol atribut específic del posseïdor de claus, i enregistrar una justificació acreditativa de la informació.

El subscriptor 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 l'EC-UR, i d'acord amb la DPC i la documentació d'operacions de l'EC-UR.

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

Adicionalment, el subscriptor 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. Els registres han d'estar a disposició de l'EC-UR en tot moment.

4.5. Lliurament i acceptació del servei

Amb la signatura del full de lliurament, el posseïdor de claus (custodi del certificat d'entitat) reconeix que se l'ha lliurat la targeta, el certificat, la clau privada i qualsevol altre suport tècnic lliurat per la Institució, així com, quan pertoqui, el codi d'identificació personal, i que aquests elements funcionen correctament.

El posseïdor de claus 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-UR.

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.,

4.6. Posseïdors de claus del subscriptor

El subscriptor s'obliga informar els posseïdors de claus dels termes i condicions relatius a l'ús dels certificats.

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

4.7. 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-UR, les claus privades i, si s'escau, les especificacions propietat de l'EC-UR 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 a l'EC-UR.

4.8. Obligacions d'ús correcte

El subscriptor ha d'utilitzar el servei de certificació CEIXSA prestat per l'EC-UR, 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 empra.

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

El subscriptor reconeixerà:

- 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.

4.9. 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-UR 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-UR 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.

Adicionalment, 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-UR, es regeix per la DPC de l'EC-UR 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 o pel posseïdor de claus, utilitzant la clau privada corresponent a la clau pública continguda al certificat CEIXSA, 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 CEIXSA 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 que 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 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 adient per verificar-la.
- Cal comprovar l'estat de revocació dels certificats de la cadena amb la informació subministrada al Registre de l'EC-UR (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 que 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 que 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 que 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-UR 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-UR 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-UR 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-UR, 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-UR, 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-UR, sense previ consentiment escrit.

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

Els serveis de certificació digital prestats per l'EC-UR 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-UR pels serveis de certificació digital

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

L'EC-UR únicament 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-UR, 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-UR 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-UR, excepte que hi hagi una declaració escrita en sentit contrari.

7. ACORDS APLICABLES, DPC.

7.1. Acords aplicables

Els acords aplicables al certificat CEIXSA, 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 l'EC-UR 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 <http://www.catcert.net/registre>.

7.3. Política de certificació

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

8. POLITICA D'INTIMITAT

L'EC-UR 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-UR 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 CEIXSA 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

L'EC-UR ha superat les següents auditories:

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