



Agència Catalana
de Certificació

CENTRE DE SUPERCOMPUTACIÓ
DE CATALUNYA



Text de divulgació del certificat CPX-2 d'Estudiant

Entitat de Certificació d'Universitats i Recerca

Referència: CPX-2 d'Estudiant-textdivulgatiu
Versió: 1.0
Data: 25/04/2005

Índex

1. INFORMACIÓ DE CONTACTE.....	4
1.1. Organització responsable.....	4
1.2. Persona de contacte	4
2. TIPUS I FINALITAT DEL CERTIFICAT CPX-2 d'Estudiant.....	4
2.1. Certificat personal de xifrat de classe 2 d'Estudiant.....	4
2.2. Entitat de Certificació emissora	5
3. LÍMITS D'ÚS	6
3.1. Límits d'ús adreçats als subscriptors.....	6
3.2. Límits d'ús adreçats als verificadors	6
4. OBLIGACIONS DELS SUBSCRIPTORS	6
4.1. Sol·licitud de certificats	6
4.2. Veracitat de la informació	7
4.3. Obligacions de custòdia.....	7
4.4. Obligacions d'ús correcte.....	7
4.5. Transaccions prohibides	8
5. OBLIGACIONS DEL VERIFICADOR.....	8
5.1. Decisió informada	8
5.2. Requeriments de verificació de la signatura electrònica	8
5.3. Diligència exigible	9
5.4. Confiança en una signatura no verificada.....	10
5.5. Efecte de la verificació.....	10
5.6. Ús correcte i activitats prohibides	10
6. GARANTIES LIMITADES I REBUIG DE GARANTIES.....	11
6.1. Garantia de l'EC-UR per als serveis de certificació digital.....	11
6.2. Exclusió de la garantia	11
7. ACORDS APLICABLES, DPC.	11
7.1. Acords aplicables	11
7.2. Declaració de pràctiques de certificació	11
8. POLITICA D'INTIMITAT.....	12



Agència Catalana
de Certificació

Text de divulgació del certificat CPX-2 d'Estudiant

9. POLITICA DE REINTEGRAMENT.....	12
10. LLEI APLICABLE, JURISDICCIO COMPETENT	12

1. INFORMACIÓ DE CONTACTE

1.1. Organització responsable

L'Entitat de Certificació d'Universitats i Recerca (EC-UR) és una iniciativa conjunta 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 CPX-2 d'Estudiant

2.1. Certificat personal de xifrat de classe 2 d'Estudiant

Els certificats personals de xifrat de classe 2 d'Estudiant (en endavant, CPX-2 d'Estudiant) no són certificats reconeguts de signatura i, en conseqüència, només es poden utilitzar per xifrar documents propis o per rebre missatges de dades

confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge per part de l'emissor del missatge utilitzant:

- a. La clau pública del posseïdor de claus indicada al CPX-2 d'Estudiant.
- b. Una clau de xifrat de sessió, simètrica, xifrada amb la clau pública del posseïdor de claus indicada al CPX-2 d'Estudiant.

El posseïdor de la clau ha d'utilitzar la seva clau privada per desxifrar el missatge.

Els CPX-2 d'Estudiant garanteixen la identitat del subscriptor però no permeten la generació de signatures electròniques de missatges.

La clau privada del CPX-2 d'Estudiant ha d'estar arxivada perquè pugui ser recuperada posteriorment, en les condicions establertes en aquest annex.

Els certificats CPX-2 d'Estudiant inclouen una manifestació relativa a la condició del posseïdor de claus, com Estudiant adscrit a un centre del subscriptor del certificat, que ha estat comprovada abans d'emetre el certificat, i és correcta i vigent mentre el certificat també es trobi vigent.

Els CPX-2 d'Estudiant emesos per l'EC-UR s'identifiquen amb l'identificador de l'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.42.2.1

2.2. Entitat de Certificació emissora

Els CPX-2 d'Estudiant són emesos per l'Entitat de Certificació d'Universitats i Recerca (EC-UR), operada per CATCert sota la direcció del CESCA, en desplegament del Conveni signat el 23 d'octubre de 2003 entre el Departament d'Universitats, Recerca i Societat de la Informació, la Fundació Catalana per a la Recerca, la Universitat de Barcelona, la Universitat Autònoma de Barcelona, la Universitat Politècnica de Catalunya, la Universitat Pompeu Fabra, la Universitat de Girona, la Universitat de Lleida, la Universitat Rovira i Virgili, la Universitat Oberta de Catalunya, l'Associació Catalana d'Entitats de Recerca, Serveis Públics Electrònics (CAT365), l'Agència Catalana de Certificació i el Consorci Centre de Supercomputació de Catalunya.

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

El CESCA pot actuar 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 CPX-2 d'Estudiant prestat per l'EC-UR exclusivament per als usos autoritzats a les Condicions Generals del Servei de Certificació Digital de Classe 1, i 2 signades entre el subscriptor i el CESCA, que es reproduïxen 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 empli.

El verificador no pot adoptar mesures d'inspecció, alteració o descompilació 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 CPX-2 d'Estudiant, i el corresponent servei d'informació, prestat per l'EC-UR, exclusivament per als usos autoritzats a les Condicions generals d'ús del certificat CPX-2 d'Estudiant, que es reproduïxen 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 empli.

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

4. OBLIGACIONS DELS SUBSCRIPTORS

4.1. Sol·licitud de certificats

El subscriptor s'ha d'obligar a realitzar les sol·licituds de certificats CPX-2 d'Estudiant 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.

4.2. Veracitat de la informació

El subscriptor s'ha de responsabilitzar 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 l'EC-UR 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.

4.3. Obligacions de custòdia

El subscriptor s'ha d'obligar 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 Virtual.

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.

4.4. Obligacions d'ús correcte

El subscriptor ha d'utilitzar el servei de certificació CPX-2 d'Estudiant 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 empri.

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

El subscriptor reconeixerà:

- a) 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.
- b) 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.

4.5. 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") 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 procedir a xifrar un missatge o document per a una persona, cal utilitzar la clau pública del destinatari. Aquesta clau pública es pot obtenir a partir del seu certificat digital CPX-2 d'Estudiant.

Per tant, és necessari verificar aquest certificat abans de procedir al xifrat.

La comprovació de la signatura electrònica del certificat és imprescindible per determinar que la clau pública continguda al certificat correspon al subscriptor i que la corresponent clau privada permet desxifrar el missatge.

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 certificació 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.

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.

- 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 xifrar missatges per a un destinatari sense haver verificat amb èxit el seu certificat.

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 dels certificats CPX de classe 2, d'acord amb aquestes condicions d'ús, el verificador pot confiar en la identificació i, en el seu cas, clau pública del posseïdor de claus, dins de les limitacions d'ús corresponents, per generar missatges xifrats.

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 exprés.

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 per als 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 no hagi comunicat el contrari mitjançant el Registre de certificació, d'acord amb la DPC.

L'EC-UR únicament garanteix que:

- a) 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 o per l'Entitat de Registre Col·laboradora, en el moment de l'emissió del certificat.
- b) Tots els certificats compleixen els requeriments formals i de contingut de la DPC.
- c) 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 xifrar, desxifrar o utilitzar d'una altra forma cap 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 CPX-2 d'Estudiant, vénen continguts a les Condicions Generals del Servei de Certificació Digital de Classe 1, i 2 signades entre el subscriptor i el CESCA, així com a 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 i 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 les pàgines <http://www.catcert.net/registre> i <http://www.cesca.es/scd>.

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 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. POLITICA DE REINTEGRAMENT

Donat el caràcter gratuït del certificat de CPX-2 d'Estudiant 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.