



**Agència Catalana
de Certificació**

Text de divulgació del certificat CEX-1

***Entitat de Certificació de la Secretaria
d'Administració i Funció Pública***

Referència:
Versió: 1.0
Data: 23/12/2004

Índex

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

8.	<i>POLITICA D'INTIMITAT</i>	11
9.	<i>POLITICA DE REINTEGRAMENT</i>	11
10.	<i>LLEI APLICABLE , JURISDICCIO COMPETENT</i>	11
11.	<i>ACREDITACIONS, SEGELLS DE QUALITAT</i>	11

1. INFORMACIÓ DE CONTACTE

1.1. Organització responsable

L'Entitat de Certificació de la Secretaria d'Administració i Funció Pública de la Generalitat de Catalunya és una iniciativa de:

CATCert – Agència Catalana de Certificació

Passatge de la Concepció, 11

08008 – Barcelona

1.2. Persona de contacte

Per a qualsevol consulta, dirigiu-vos a:

CATCert – Agència Catalana de Certificació

Àrea d'assessorament i recerca

Passatge de la Concepció, 11

08008 – Barcelona

2. TIPUS I FINALITAT DEL CERTIFICAT CEX-1

2.1. Certificat d'Entitat de Xifrat de classe 1

Els certificats d'entitat de xifrat de classe 1 (en endavant, CEX-1) són certificats reconeguts d'acord amb el que s'estableix a l'article 7 i 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 CEX-1 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 CEX-1 garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten xifrar documents i 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 CEX-1.
- b. Una clau de xifrat de sessió, simètrica, xifrada amb la clau pública del posseïdor de claus indicada al CEX-1 .

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

Els CEX-1 garanteixen la identitat del subscriptor però no permeten la generació de signatures electròniques de missatges.

La clau privada del CEX-1 ha d'estar arxivada perquè pugui ser recuperada posteriorment, en les condicions establertes en aquest annex.

Els CEX-1 emesos per l'EC-SAFP s'identifiquen amb l'identificador de l'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.131.

2.2. Entitat de Certificació emissora

Els CEX-1 són emesos per l'Entitat de Certificació SAFP de la Secretaria d'Administració i Funció Pública, operada per CATCert.

CATCert és el prestador de serveis de certificació que emet els certificats de l'EC-SAFP, 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 CEX-1 prestat per l'EC-SAFP 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-SAFP.

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

3.2. Límits d'ús adreçats als verificadors

El verificador ha d'utilitzar el servei de certificació CEX-1, i el corresponent servei d'informació, prestat per l'EC-SAFP, exclusivament per als usos autoritzats a les "Condicions generals d'ús del certificat CEX-1", 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-SAFP.

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

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

4. OBLIGACIONS DELS SUBSCRIPTORS

4.1. Generació de claus

El subscriptor autoritza a l'EC-SAFP a 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 CEX-1.

4.2. Sol·licitud de certificats

El subscriptor 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 l'EC-SAFP, d'acord amb el que s'estableix a la DPC i a la documentació d'operacions de l'EC-SAFP.

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

4.5. Obligacions d'ús correcte

El subscriptor ha d'utilitzar el servei de certificació CEX-1 prestat per l'EC-SAFP, 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 1 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.

4.6. 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-SAFP per realitzar cap transacció prohibida per la llei aplicable.

Els serveis de certificació digital prestats per l'EC-SAFP 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-SAFP 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-SAFP, es regeix per la DPC de l'EC-SAFP 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 pròpia o la del destinatari. Aquesta clau pública es pot obtenir a partir del seu certificat digital CEX-1.

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 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-SAFP (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.

5.3. Confiança en un certificat no verificat

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

Si el verificador confia en un certificat no verificat, assumirà tots els riscos derivats d'aquesta actuació.

5.4. Efecte de la verificació

En virtut de la correcta verificació del certificats CEX de classe 1, 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.

5.5. 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-SAFP, 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-SAFP, sense previ consentiment escrit.

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

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

L'EC-SAFP garanteix que:

- a) la clau privada de l'entitat de certificació utilitzada per emetre certificats no ha estat compromesa, llevat que l'EC-SAFP no hagi comunicat el contrari mitjançant el Registre de certificació, d'acord amb la DPC.
- 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-SAFP, 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-SAFP no garanteix cap programari que utilitzi qualsevol persona per xifrar, desxifrar o utilitzar d'una altra forma cap certificat digital emès per l'EC-SAFP, excepte que hi hagi una declaració escrita en sentit contrari.

7. ACORDS APLICABLES, DPC.

7.1. Acords aplicables

Els acords aplicables al certificat CEX-1, 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-SAFP 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-SAFP disposa d'una política de certificació que detalla els requisits de caràcter tècnic, jurídic, operatiu, així com de regulació del certificat CEX-1, a disposició de la comunitat d'usuaris que la sol·licitin.

8. POLITICA D'INTIMITAT

L'EC-SAFP 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-SAFP 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 CEX-1 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-SAFP ha superat les següents auditories:

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