UNIVERSITAT ROVIRA I VIRGILI

Declaració de Pràctiques de Certificació

Entitat de Certificació de la Universitat Rovira i Virgili

Referència: D1111_E0650_N–DPC–009_EC-URV
Versió: 1.1
Data: 15/01/2007

Índex

1. Introducció

1.1 Presentació

El Departament d'Universitats, Recerca i Societat de la Informació (DURSI), la Fundació Catalana per a la Recerca i la Innovació (FCRI), les universitats públiques (UB, UAB, UPC, UPF, UdG, URV i UdL), la universitat no presencial (UOC), l'Associació Catalana d'Entitats de Recerca (ACER), l'Administració Oberta de Catalunya (AOC), l'Agència Catalana de Certificació (CATCert) i el Centre de Supercomputació de Catalunya (CESCA), van signar un conveni el 23 d'octubre de 2003 amb l'objectiu que les universitats i centres de recerca incorporin la signatura digital per incrementar la seguretat de les seves comunicacions telemàtiques.

El 26 de maig de 2005 es va signar el conveni per a la creació i gestió de l'Entitat de Certificació de la Universitat Rovira i Virgili (EC-URV). L'EC-URV és una Entitat de Certificació Vinculada a l'Entitat de Certificació d'Universitats i Recerca (EC-UR), titularitat del CESCA, que al mateix temps és una Entitat de Certificació Vinculada a la jerarquia d'Entitats de Certificació de les entitats públiques de Catalunya. L'EC-URV és titularitat de la URV operada per CATCert sota la direcció del CESCA .

La URV actua com Entitat de Registre Interna, de forma que, com a subscriptora dels certificats, registra directament els seus posseïdors de claus. També realitza la validació i l'aprovació interna i prèvia de les sol·licituds de certificats i, quan sigui necessari, sol·licita la suspensió, revocació o renovació de certificats.

1.1.1 Tipus i classes de certificats

L'Agència Catalana de Certificació ha definit una tipologia de serveis de certificació, que permeten a l'EC-URV emetre certificats digitals per a diversos usos, i usuaris finals diferents.

Els certificats d'usuaris finals es divideixen en:

- Certificats personals, caracteritzats pel fet que el posseïdor de la clau privada és una persona física, que actua en el seu propi nom i representació, o en representació i per compte del subscriptor.
- Certificats d'entitat, caracteritzats pel fet que el subscriptor del certificat i, d'acord amb la llei, el signant, és una persona jurídica, que actua per mitjà d'un posseïdor de claus.
- Certificats de dispositiu, caracteritzats pel fet el posseïdor de la clau privada és un dispositiu informàtic que realitza operacions de signatura i desxifrat de forma automàtica, sota la responsabilitat del subscriptor.

Els certificats d'usuari final s'emeten en dues modalitats: de classe 1 i de classe 2. Els certificats de classe 1 són certificats d'organització del sector públic de Catalunya (corporatius) que es caracteritzen pel fet de que el posseïdor de claus té una vinculació amb el subscriptor o titular del certificat, que és una persona jurídica; mentre que, els certificats de classe 2 són la resta de certificats no inclosos en la definició anterior. Aquests últims es subdivideixen, a la vegada, en individuals o col·lectius en funció de si s'expedeixen a una

persona física que actua en nom propi, o a una organització que actua per mitjà d'una persona física.

1.1.1.1 Certificats personals

L'EC-URV emet vuit tipus de certificats personals:

- Certificats personals d'identitat i de signatura electrònica reconeguda de classe 1 amb càrrec (CPISR-1 Càrrec), que identifiquen la persona que els posseeix, la seva organització subscriptora, i el seu càrrec en aquesta, i que serveixen per signar missatges amb dispositiu segur de creació de firma, així com missatges d'autenticació i d'accés segur a sistemes informàtics.
- Certificats personals d'identitat i de signatura electrònica reconeguda de classe 1 amb càrrec per estrangers (CPISR-1 Càrrec Estranger), que identifiquen la persona que els posseeix, la seva organització subscriptora, i el seu càrrec en aquesta, i que serveixen per signar missatges amb dispositiu segur de creació de firma, així com missatges d'autenticació i d'accés segur a sistemes informàtics.
- Certificats personals de xifrat (CPX-1 Càrrec), que identifiquen la persona que els posseeix, la seva organització subscriptora, i el seu càrrec en aquesta, i que s'utilitzen per rebre missatges confidencials.
- Certificats personals de xifrat per estranger (CPX-1 Càrrec Estranger), que identifiquen la persona que els posseeix, la seva organització subscriptora, i el seu càrrec en aquesta, i que s'utilitzen per rebre missatges confidencials.
- Certificats personals d'identitat i de signatura electrònica reconeguda de classe 2 per estudiants (CPISR-2 d'Estudiant), que identifiquen la persona que els posseeix, la seva organització subscriptora, i la seva condició d'estudiant, i que serveixen per signar missatges amb dispositiu segur de creació de firma, així com missatges d'autenticació i d'accés segur a sistemes informàtics.
- Certificats personals d'identitat i de signatura electrònica reconeguda de classe 2 per estudiants estrangers (CPISR-2 d'Estudiant Estranger), que identifiquen la persona que els posseeix, la seva organització subscriptora, i la seva condició d'estudiant, i que serveixen per signar missatges amb dispositiu segur de creació de firma, així com missatges d'autenticació i d'accés segur a sistemes informàtics.
- Certificats personals de xifrat per estudiants (CPX-2 d'Estudiant), que identifiquen la persona que els posseeix, la seva organització subscriptora, i la seva condició d'estudiant, i que s'utilitzen per rebre missatges confidencials
- Certificats personals de xifrat per estudiant estranger (CPX-2 d'Estudiant Estranger), que identifiquen la persona que els posseeix, la seva organització subscriptora, i la seva condició d'estudiant, i que s'utilitzen per rebre missatges confidencials.

El certificat personal de identificació i signatura reconeguda de classe 1 amb càrrec (CPISR-1 Càrrec), i amb càrrec per estrangers (CPISR-1 Càrrec Estranger), és un certificat reconegut d'acord amb l'establert a l'article 11.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, amb el contingut prescrit per l'article 11.2, i emès complint les obligacions dels articles 12, 13, 18 i 20 de la Llei esmentada. Funciona 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 dona compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. Garanteix la identitat del subscriptor i del posseïdor de la clau privada d'identificació i firma, i permet 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 utilitzant un dispositiu segur de creació de signatura, per la qual cosa, de conformitat 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 compliment de cap requisit addicional. A més d'això, inclou una manifestació relativa a la categoria de personal i al càrrec del posseïdor de claus, que ha estat comprovada abans d'emetre el certificat, i és correcta. Tanmateix, 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 del certificat. També es pot utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura escrita, sinó només la identificació del posseïdor de claus.

El certificat personal de xifrat de classe 1 amb càrrec (CPX-1 Càrrec), i amb càrrec per estrangers (CPX-1 Càrrc Estranger), no és un certificat reconegut de signatura electrònica i, en conseqüència, només es pot utilitzar per xifrar documents propis o per rebre documents confidencials, en qualsevol format, protegits mitjançant el xifrat del document per part de l'emissor del missatge utilitzant, bé la clau pública del posseïdor de claus indicada al certificat, o bé una clau de xifrat de sessió, simètrica, xifrada amb clau pública del posseïdor de claus indicada en el certificat. Garanteixen la identitat del subscriptor però no permet la generació de signatures electròniques de missatges. A més, inclou una manifestació relativa a la categoria de personal i al càrrec del posseïdor de claus, que ha estat comprovada abans d'emetre el certificat i és correcte.

El certificat personal de identificació i signatura reconeguda de classe 2 per a estudiants (CPISR-2 d'Estudiant), i a per estudiants estrangers (CPISR-2 d'Estudiant Estranger), és un certificat reconegut d'acord amb l'establert a l'article 11.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, amb el contingut prescrit per l'article 11.2, i emès complint les obligacions dels articles 12, 13, 18 i 20 de la Llei esmentada. Funciona 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 dona compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. Garanteix la identitat del subscriptor i del posseïdor de la clau privada d'identificació i firma, 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 utilitzant un dispositiu segur, per la qual cosa, de conformitat 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 amb cap requisit addicional. A més d'això, inclou una manifestació relativa a la condició d'estudiant adscrit a un centre del subscriptor del certificat, que ha estat comprovada abans d'emetre el certificat, i és correcta. També es pot utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura escrita, sinó només la identificació del posseïdor de claus.

El certificat personal de xifrat de classe 2 per a estudiant (CPX-2 d'Estudiant), i per a estudiant estranger (CPISR-2 d'Estudiant Estranger), no és un certificat reconegut de signatura electrònica i, en conseqüència, només es pot utilitzar per xifrar documents propis o per rebre documents confidencials, en qualsevol format, protegits mitjançant el xifrat del document per part de l'emissor del missatge utilitzant, bé la clau pública del posseïdor de

claus indicada al certificat, o bé una clau de xifrat de sessió, simètrica, xifrada amb clau pública del posseïdor de claus indicada en el certificat. Garanteixen la identitat del subscriptor però no permet la generació de signatures electròniques de missatges. A més, inclou una manifestació relativa a la condició d'estudiant adscrit a un centre del subscriptor del certificat, que ha estat comprovada abans d'emetre el certificat, i és correcta.

Els certificats CPISR-1 i CPX-1, i els certificats CPISR-2 i CPX-2, s'emeten conjuntament, dins de la targeta del posseïdor de claus, que té la consideració de dispositiu segur de creació de signatura .

1.1.1.2 Certificats d'entitat

L'EC-URV emet dos tipus de certificats d'entitat:

- Certificats d'entitat de signatura electrònica reconeguda (CESR), d'acord amb l'establert en l'article 7 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, que permet que Institucions públiques i privades, corporacions de dret públic i persones juridico-públiques (col·lectivament anomenades "entitats") signin documents amb dispositiu segur de creació de signatura, missatges d'autenticació (confirmació de la identitat) i d'accés segur a sistemes informàtics.
- Certificats d'entitat de xifrat (CEX), d'acord amb l'establert en l'article 7 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, que permet que Institucions públiques i privades, corporacions de dret públic i persones juridico-públiques (col·lectivament anomenades "entitats") puguin produir i rebre documents confidencials

Els certificats d'entitat no admeten combinacions, expedint-se sempre per separat.

Addicionalment, en funció dels requeriments tècnics i de les necessitats dels usuaris, es possible que aquests tipus de certificats puguin incorporar altres funcionalitats que, en tot cas, seran identificades en una política específica de certificació, que serà desenvolupada o aprovada per CATCert.

1.1.1.3 Certificats de dispositiu

L'EC-URV emet quatre tipus de certificats de dispositiu:

- Certificat de dispositiu servidor segur (CDS), que s'utilitza per una aplicació informàtica, servidor de SSL o de TLS, perquè s'identifiqui davant de les aplicacions client que es connecten i per protegir el secret de les comunicacions entre el client i el servidor.
- Certificat de dispositiu segur de controlador de domini (CDSCD), s'utilitza per una aplicació informàtica servidor SSL o TLS, per autenticar en una xarxa windows als usuaris que pertanyen a un determinat domini, mitjançant un certificat digital de signatura amb targeta criptogràfica.
- Certificat de dispositiu d'aplicació digitalment assegurada (CDA), que és utilitzat per aplicacions informàtiques que s'identifiquen digitalment, signen electrònicament *webservices* o altres protocols i que reben document i missatges xifrats.

- Certificat de signatura d'aplicacions informàtiques (CDP), que serveix per signar electrònicament les aplicacions informàtiques a transmetre a través de xarxes o d'Internet.

Addicionalment, en funció dels requisits tècnics i les necessitats dels usuaris, és possible que els esmentats tipus de certificats puguin incorporar altres funcionalitats que, en tot cas, seran identificades en una política específica de certificació, que haurà de ser aprovada per CATCert.

1.1.2 Relació entre la Declaració de pràctiques de certificació i altres documents

Aquest document conté la declaració de pràctiques de certificació de l'EC-URV.

L'EC-URV emet certificats dins de la Jerarquia de l'Agència Catalana de Certificació, per tant ha de disposar d'una declaració de pràctiques de certificació d'acord amb la política general de certificació de CATCert i, en el seu cas, amb la política específica de certificació de l'EC-URV.

Aquesta Declaració de Pràctiques de Certificació (DPC) inclou els procediments que aplica l'EC-URV en la prestació dels seus serveis, en compliment dels requisits establerts per les polítiques que gestiona i l'article 19 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

1.2 Nom del document i identificació

1.2.1 Identificació d'aquest document

Aquest document es denomina "Declaració de Pràctiques de Certificació (DPC) de l'EC-URV".

Aquesta Declaració de Pràctiques de Certificació s'identifica amb el següent OID:

1.3.6.1.4.1.15096.1.2.9

1.2.2 Identificació de polítiques de certificació cobertes per aquesta DPC

L'EC-URV emet i gestiona certificats d'acord amb les següents polítiques:

- **CPISR Càrrec d'URV** - Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec, emès per l'EC-URV
  Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.2.3
- **CPISR Càrrec Estranger d'URV** – Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec per estrangers, emès per l'EC-URV

  Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.1.2
- **CPX Càrrec d'URV** - Certificat personal de xifrat amb càrrec, emès per l'EC-URV
  Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.41.1.3
- **CPX Càrrec Estranger d'URV** – Certificat personal de xifrat amb càrrec per estrangers, emès per L'EC-URV

  Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.41.2.2
- **CPISR d'Estudiant** - Certificat personal d'identificació i signatura electrònica reconeguda per estudiant, emès per l'EC-URV

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.82.2.2

- **CPISR d'Estudiant Estranger** – Certificat personal d'identificació i signatura electrònica reconeguda per estudiant estranger, emès per l'EC-URV

  Classe 2. OID: 1.3.6.1.4.1.15096. 1.3.1.82.2.4

- **CPX d'Estudiant d'URV** - Certificat personal de xifrat d'estudiant, emès per l'EC-URV
  Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.42.2.2

- **CPX d'Estudiant Estranger d'URV** – Certificat personal de xifrat d'estudiant estranger, emès per l'URV

  Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.42.2.4

- **CESR** – Certificat d'entitat de signatura electrònica reconeguda, emès per l'EC-URV.
  Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.121.5

- **CEX** – Certificat d'entitat de xifrat emès per l'EC-URV
  Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.131.5

- **CDS** - Certificat de dispositiu servidor segur, emès per l'EC-URV
  Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51

- **CDA** - Certificat de dispositiu d'aplicació digitalment assegurada, emès per l'EC-URV
  Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.91

- **CDP** - Certificat de dispositiu de signatura de programari, emès per l'EC-URV
  Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.71

- **CDSCD** – Certificat de dispositiu segur de controlador de domini, emès per l'EC-URV

  Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.1

1.3 Comunitat d'usuaris de certificats

Aquesta declaració de pràctiques de certificació regula una comunitat d'usuaris, que obtenen certificats per a diverses relacions administratives i privades, d'acord amb la Llei 59/2003 i la normativa administrativa corresponent.

Els certificats de l'EC-URV no s'expedeixen al públic, sinó al personal, als estudiants i als dispositius de les facultats i els centres universitaris de la Universitat Rovira i Virgili.

1.3.1 Prestadors de serveis de certificació

Un prestador de serveis de certificació és una persona física o jurídica que produeix certificats i presta altres serveis en relació amb la signatura electrònica, d'acord amb la Llei 59/2003, de 19 de desembre, de signatura electrònica.

El prestador de serveis de certificació genera els certificats digitals mitjançant l'operació d'entitats de certificació de la seva titularitat, que firmen els certificats.

CATCert és el prestador de serveis de certificació de la Universitat Rovira i Virgili, amb la corresponent Autoritat de Certificació diferenciada i vinculada a la jerarquia d'entitats de certificació de les entitats públiques de Catalunya.

En la seva funció de prestador de serveis de certificació, CATCert es responsable, davant dels usuaris finals i, en especial, dels tercers verificadors de certificats i firmes electròniques, per l'actuació de les autoritats de certificació que operen en nom de les diferents entitats de certificació.

Aquesta funció d'Entitat de Certificació s'entén sense perjudici de la possibilitat que la Universitat Rovira i Virgili actuï com prestador de serveis de certificació, vinculats o no a la jerarquia pública de certificació de Catalunya.

1.3.2 Entitat de Certificació Arrel

L'Entitat de Certificació Arrel és CATCert, que disposa d'una autoritat de certificació principal, anomenada "Arrel de la jerarquia pública de certificació de Catalunya", que té la finalitat d'integrar altres entitats de certificació al sistema públic català de certificació mitjançant la vinculació tècnica de les autoritats de certificació corresponents.

1.3.3 EC-UR

El Departament d'Universitats, Recerca i Societat de la Informació (DURSI), la Fundació Catalana per a la Recerca i la Innovació (FCRI), les universitats públiques (UB, UAB, UPC, UPF, UdG, URV i UdL), la universitat no presencial (UOC), l'Associació Catalana d'Entitats de Recerca (ACER), l'Administració Oberta de Catalunya (AOC), l'Agència Catalana de Certificació (CATCert) i el Centre de Supercomputació de Catalunya (CESCA), van signar un conveni el 23 d'octubre de 2003 amb l'objectiu que les universitats i centres de recerca incorporin la signatura digital per incrementar la seguretat de les seves comunicacions telemàtiques mitjançant la creació de l'EC-UR, vinculada a la jerarquia d'entitats de certificació de les entitats públiques de Catalunya, que emet els certificats a la URV.

1.3.4 EC-URV

En acord del Consell de Govern de la URV de data 23 de febrer de 2006 es va aprovar la implantació a la Universitat Rovira i Virgili de la política de clau pública, constituint-se la URV com a autoritat de certificació d'acord amb la Llei 59/2003, de 19 de desembre, de signatura electrònica i la resta de normativa aplicable.

El 26 de maig de 2005 es va signar el conveni per a la creació i gestió de l'Entitat de Certificació de la Universitat Rovira i Virgili (EC-URV), de la qual és titular la Universitat Rovira i Virgili. L'EC-URV és una Entitat de Certificació Vinculada a l'Entitat de Certificació d'Universitats i Recerca (EC-UR), titularitat del CESCA, que al mateix temps és una Entitat de Certificació Vinculada a la jerarquia d'Entitats de Certificació de les entitats públiques de Catalunya.

1.3.5 Entitats de Registre

Les Entitats de Registre són persones físiques o jurídiques que assisteixen a les Entitats de Certificació en determinats procediments i relacions amb els sol·licitants i subscriptors de certificats, especialment en els tràmits d'identificació, registre i autenticació dels subscriptors dels certificats i dels posseïdors de claus.

La Universitat Rovira i Virgili, com a Entitat de Registre Interna (ERI), dissenya i implanta els components i procediments tècnics, jurídics i de seguretat, referents als cicles de vida dels dispositius segurs de creació de signatura o, quan s'escaigui, xifrat; al cicle de vida de les claus en programari i al cicle de vida dels certificats que emetin.

1.3.6 Usuaris finals

Els usuaris finals són les persones que obtenen i utilitzen els certificats emesos per l'EC-URV, i, en concret, podem distingir els següents usuaris finals:

- Els sol·licitants de certificats (la URV)
- Els subscriptors de certificats i els posseïdors de claus.
- Els verificadors de signatures i dels certificats

1.3.6.1 Sol·licitants de certificats

Els sol·licitants dels certificats indicats en aquest document són persones autoritzades per la Universitat Rovira i Virgili (URV).

1.3.6.2 Subscriptors de certificats

El subscriptor dels certificats és la URV, que s'identifica als certificats.

El subscriptor actua sempre mitjançant els posseïdors de les claus, persones físiques que es troben degudament autoritzades per rebre els certificats, i que també figuren identificades als certificats.

1.3.6.3 Posseïdors de claus

Els posseïdors de les claus poden, per tant, signar, xifrar i desxifrar missatges i documents del subscriptor.

Els posseïdors de claus dels certificats de classe 1 de la URV són el personal al seu servei, incloent-hi professors i personal d'administració.

Els posseïdors de claus dels certificats de classe 2 de la URV són els estudiants.

1.3.6.4 Verificadors de certificats

Els verificadors són les persones, les organitzacions i les combinacions dels anteriors que reben signatures digitals i certificats digitals i han de verificar-los, com pas previ a confiar.

1.4 Ús dels certificats

Aquesta secció llista les aplicacions per a les quals pot utilitzar-se cada tipus de certificat, establint limitacions i prohibeix algunes aplicacions dels certificats.

1.4.1 Usos típics dels certificats

1.4.1.1 Certificats personals d'identificació i signatura electrònica reconeguda de classe 1 amb càrrec (CPISR-1 Càrrec) i amb càrrec per estrangers (CPISR-1 Càrrec Estrangers)

Els certificats personals d'identificació i signatura reconeguda de classe 1 amb càrrec, i amb càrrec per estrangers, són certificats reconeguts d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emès complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que

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

Aquests 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.

Per aquest motiu, aquests certificats garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i firma, 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 utilitzant 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.

Aquests certificats inclouen una manifestació relativa a la categoria de personal i càrrec del posseïdor de claus, que ha estat comprovada abans d'emetre el certificat, i és correcta, quan ho prevegi una política específica.

A més es poden utilitzar per a diversos usos, entre els quals es poden indicar els següents:

- Identificació en servidors web basada en presentació del certificat.
- Autenticació en sistemes de control d'accés, de sistema operatiu o centralitzats.

1.4.1.2 Certificats personals d'identificació i signatura electrònica reconeguda de classe 2 d'estudiant (CPISR-2 Estudiant) i d'estudiant estranger (CPISR-2 d'Estudiant Estranger)

Els certificats personals d'identificació i signatura reconeguda de classe 2 d'estudiant, i d'estudiant estranger, són certificats reconeguts d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emès complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Aquests 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.

Per aquest motiu, aquests certificats 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 utilitzant 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.

Aquests certificats inclouen una manifestació relativa a la condició del posseïdor de claus, com estudiant adscrit a un centre del subscriptor del certificat, que han estat comprovats abans d'emetre el certificat, i són correctes i vigents mentre el certificat també es troba vigent.

A més es poden utilitzar per a diversos usos, entre els quals es poden indicar els següents:

- Identificació en servidors web basada en presentació del certificat.
- Autenticació en sistemes de control d'accés, de sistema operatiu o centralitzats.

1.4.1.3 Certificats personals de xifrat de classe 1 amb càrrec (CPX-1 Càrrec) i amb càrrec per estrangers (CPX-1 Càrrec Estrangers)

Els certificats personals de xifrat són certificats ordinaris que s'utilitzen exclusivament per rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, per part del remitent del missatge.

El posseïdor de la clau utilitza la seva clau privada per desxifrar el missatge. Aquests certificats garanteixen la identitat del subscriptor, però no permeten la signatura electrònica de missatges de dades.

La clau privada d'aquests certificats pot estar arxivada per l'entitat de certificació de manera que, en certes circumstàncies, pugui recuperar-se i accedir a la informació xifrada, fins i tot sense la intervenció del subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització.

1.4.1.4 Certificats personals de xifrat de classe 2 d'estudiant (CPX-2 Estudiant) i d'estudiant estranger (CPX-2 d'Estudiant Estranger)

Els certificats personals de xifrat són certificats ordinaris que s'utilitzen exclusivament per rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, per part del remitent del missatge.

El posseïdor de la clau utilitza la seva clau privada per desxifrar el missatge. Aquests certificats garanteixen la identitat del subscriptor, però no permeten la signatura electrònica de missatges de dades.

La clau privada d'aquests certificats pot estar arxivada per l'entitat de certificació de manera que, en certes circumstàncies, pugui recuperar-se i accedir a la informació xifrada, fins i tot sense la intervenció del subscriptor o del posseïdor de claus.

Aquests certificats 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.

El posseïdor de la clau utilitza la seva clau privada per a desxifrar els missatges.

1.4.1.5 Certificats d'Entitat de Signatura Reconeguda (CESR)

Els certificats d'entitat de signatura reconeguda 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 emès complint les obligacions dels articles 7, 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de firma electrònica, i que donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Aquests són certificats reconeguts que funcionen amb dispositiu segur de creació de firma electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre.

Per aquest motiu, aquests certificats garanteixen la identitat del subscriptor i del posseïdor de la clau privada de signatura, essent idonis per a oferir suport a la signatura electrònica reconeguda de l'entitat; això és la firma electrònica avançada que es basa en un certificat reconegut i que ha estat generada utilitzant un dispositiu segur, per la qual cosa, d'acord amb el que estableix l'article 3.4 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.

1.4.1.6 Certificat d'entitat de xifrat (CEX)

Els certificats de entitat de xifrat són certificats ordinaris, que s'expedeixen a subscriptors i s'utilitzen exclusivament per xifrar o rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, utilitzant la clau pública del subscriptor indicada al CEX.

Els CEX corresponen a certificats amb dispositiu segur de creació de signatura electrònica, per al desxifrat, no expedits al públic, d'acord amb el document ETSI TS 101 456 v1.1.1.

El posseïdor de la clau utilitza la seva clau privada per a desxifrar els missatges.

1.4.1.7 Certificats de dispositiu de servidor segur (CDS)

Els CDS s'emeten a les facultats i els centres universitaris de la Universitat Rovira i Virgili, responsables de l'operació de servidors segurs SSL o TLS, amb els següents usos:

- Autenticació de servidor
- Xifrat de les comunicacions entre client i servidor

Aquests són certificats ordinaris, i que garanteixen la identitat de la persona responsable i dels servidors concrets on funcionen.

1.4.1.8 Certificats de dispositiu segur de controlador de domini (CDSCD)

Els CDSCD s'emeten a les facultats i els centres universitaris de la Universitat Rovira i Virgili responsables de l'operació deL controlador de domini, amb els següents usos:

- Autenticació del servidor
- Autenticació de l'usuari amb targeta criptogràfica

Els CDSCD són certificats ordinaris que garanteixen la identitat de la persona responsable, dels servidors concrets on funcionen i dels usuaris amb targeta criptogràfica que autentica.

1.4.1.9 Certificats de dispositiu d'Aplicació digitalment assegurada (CDA)

Els CDA s'emeten a les facultats i els centres universitaris de la Universitat Rovira i Virgili responsables de l'operació d'aplicacions informàtiques que s'identifiquen digitalment, que signa electrònicament webservices o altres protocols i que rep documents i missatges xifrats.

Són certificats ordinaris, que garanteixen la identitat de la persona responsable i la integritat i l'autenticitat de les dades firmades. També permeten la recepció d'informació xifrada.

La clau privada del CDA pot estar arxivada per l'entitat de certificació de manera que, en certes circumstàncies, pugui recuperar-se i accedir a la informació xifrada, fins i tot sense la intervenció del subscriptor.

1.4.1.10 Certificats de dispositiu de signatura de programari (CDP)

Els CDP s'emeten persones jurídiques responsables de l'edició, publicació o distribució digitals de programari informàtic, per a la signatura del programari, que permet instal·lar-lo o executar-lo a distància.

Aquests són certificats ordinaris, i que garanteixen la identitat de la persona responsable i l'origen i la integritat del programari firmat.

1.4.2 Aplicacions prohibides

1.4.2.1 Informacions per a tots els tipus de certificats

Els certificats no s'han dissenyat, no es poden destinar i no s'autoritza el seu ús o revenda com equips de control de situacions perilloses o per a usos que requereixin actuacions a prova d'errors, com al funcionament d'instal·lacions nuclears, sistemes de navegació o comunicacions aèries, o sistemes de control d'armament, on un error pogués directament comportar la mort, lesions personals o danys mediambientals severs.

1.4.2.2 Certificats personals d'identificació i signatura electrònica reconeguda.

Els certificats CPISR-1 Càrrec, CPISR-1 Càrrec Estrangers, CPISR-2 d'Estudiant i CPISR-2 d'Estudiant Estranger, no poden utilitzar-se per a:

- Signar peticions d'emissió, renovació, suspensió o revocació de certificats.
- Signar certificats de clau pública de cap tipus, ni llistes de revocació de certificats (LRC).
- Xifrar ni desxifrar missatges o documents.

1.4.2.3 Certificats personals de xifrat.

Els CPX-1 Càrrec, CPX-1 Càrrec Estrangers, CPX-2 d'Estudiant i CPX-2 d'Estudiant Estranger no poden utilitzar-se per generar signatures digitals de cap tipus de missatge de dades.

1.4.2.4 Certificats d'entitat de signatura electrònica reconeguda

Els certificats no poden utilitzar-se per a:

- Signar peticions d'emissió, renovació, suspensió o revocació de certificats.
- Signar certificats de clau pública de cap tipus, ni llistes de revocació de certificats (LRC).
- Xifrar ni desxifrar missatges o documents.

1.4.2.5 Certificats d'entitat de xifrat

Els CEX no poden utilitzar-se per generar signatures digitals de cap tipus de missatge de dades.

1.4.2.6 Certificats de dispositiu de servidor segur

Els CDS no poden utilitzar-se per signar peticions d'emissió, renovació, suspensió o revocació de certificats CIC, certificats de cap tipus o llistes de revocació de certificats (LRC).

1.4.2.7 Certificats de dispositiu de segur de controlador de domini

Els CDS no poden utilitzar-se per signar peticions d'emissió, renovació, suspensió o revocació de certificats CIC, certificats de cap tipus o llistes de revocació de certificats (LRC).

1.4.2.8 Certificats de dispositiu de signatura de programari

Sense estipulació addicional.

1.4.2.9 Certificats de dispositiu d'aplicació digitalment assegurada

Els CDA no poden utilitzar-se per signar peticions d'emissió, renovació, suspensió o revocació de certificats CIC, certificats de cap tipus, o llistes de revocació de certificats (LRC).

Tampoc no poden utilitzar-se per assegurar aplicacions diferents a la identificada al certificat.

1.5 Administració de la Declaració de Pràctiques.

1.5.1 Organitzacions que administren l'especificació

Direcció Postal:	
Universitat Rovira i Virgili Carrer de l'Escorxador, s/n 43003 Tarragona	Agència Catalana de Certificació Passatge de la Concepció, 11 08008 Barcelona
Direcció web:	
http://www.urv.net *http://www.urv.net/scd* (informació sobre subscripcions)	*http://www.catcert.net*
Telèfon:	
+34 977 55 80 00	+34 93 272 26 00
Correu-e:	
suport.scd@urv.net (informació sobre subscripcions)	*info@catcert.net*

Fax:	
+34 977 55 80 22	+34 93 272 25 39

1.5.2 Dades de contacte de les organitzacions

Direcció Postal:	
Universitat Rovira i Virgili Carrer de l'Escorxador, s/n 43003 Tarragona	Agència Catalana de Certificació Passatge de la Concepció, 11 08008 Barcelona
Direcció web:	
http://www.urv.net *http://www.urv.net/scd* (informació sobre subscripcions)	*http://www.catcert.net*
Telèfon:	
+34 977 55 80 00	+34 93 272 26 00
Correu-e:	
suport.scd@urv.net (informació sobre subscripcions)	*info@catcert.net*
Fax:	
+34 977 55 80 22	+34 93 272 25 39

1.5.3 Persones que determinen la conformitat d'una DPC amb la política

Direcció Postal:	
Universitat Rovira i Virgili Carrer de l'Escorxador, s/n 43003 Tarragona	Agència Catalana de Certificació Passatge de la Concepció, 11 08008 Barcelona

Direcció web:	
http://www.urv.net *http://www.urv.net/scd* (informació sobre subscripcions)	http://www.catcert.net
Telèfon:	
+34 977 55 80 00	+34 93 272 26 00
Correu-e:	
suport.scd@urv.net (informació sobre subscripcions)	*info@catcert.net*
Fax:	
+34 977 55 80 22	+34 93 272 25 39

1.5.4 Procediment d'aprovació

El sistema documental i d'organització de l'EC-URV garanteix, mitjançant l'existència i l'aplicació dels corresponents procediments, el correcte manteniment de la Declaració de pràctiques de certificació i de les especificacions de servei relacionades amb ella.

Es preveu, d'aquesta manera, el procediment de modificació d'especificació del servei i el procediment de publicació d'especificacions de servei. Les modificacions finals de la Declaració de Pràctiques de Certificació (DPC) són aprovades pel Consell de Govern de la Universitat Rovira i Virgili, i definitivament per l'Agència Catalana de Certificació, després de comprovar el compliment dels requisits establerts a les seccions corresponents d'aquesta DPC.

2. Publicació d'informació i dipòsit de certificats

2.1 Dipòsit de certificats

El servei de Dipòsit de certificats està disponible durant les 24 hores dels 7 dies de la setmana i, en cas d'error del sistema fora de control de l'EC-URV, aquesta realitza els seus millors esforços perquè el servei es trobi disponible de nou en el termini establert a la secció 5.7.4.

2.2 Publicació d'informació de l'EC-URV

L'EC-URV publica les següents informacions, en el seu Dipòsit:

a. Un directori actualitzat de certificats en el que s'indiquen els certificats expedits i si estan vigents, o si la seva vigència ha estat suspesa, o extingida.

b. Les llistes de certificats revocats i altres informacions d'estat de revocació dels certificats.

c. La política general de certificació i, quan sigui convenient, les polítiques específiques.

d. Els perfils dels certificats i de les llistes de revocació dels certificats.

e. La Declaració de Pràctiques de Certificació.

f. Els instruments jurídics vinculants amb subscriptors i verificadors.

Tot canvi en les especificacions o condicions del servei es comunica als usuaris per part de l'EC-URV, a través del dipòsit.

En tots els casos es fa una referència explícita als canvis a la pàgina principal del Web del servei.

No es retira la versió anterior del document objecte del canvi, però s'indica que ha estat substituït per la versió nova.

2.3 Freqüència de publicació

La informació de l'EC-URV es publica quan es troba disponible i en especial, de forma immediata quan s'emeten les mencions relatives a la vigència dels certificats.

Els canvis en aquest document es regeixen per l'establert a la secció 9.12.1

La informació d'estat de revocació de certificats es publica d'acord amb l'establert a la secció 4.9.7

Al cap de 15 (quinze) dies des de la publicació de la nova versió, es retira la referència al canvi de la pàgina principal i s'insereix en el dipòsit.

Les versions antigues de la documentació són conservades, per un període de 15 (quinze) anys per l'EC-URV, podent ser consultada, per causa raonada pels interessats.

2.4 Control d'accés

L'EC-URV no limita l'accés de lectura a les informacions establertes a la secció corresponent, però estableix controls per mantenir la integritat del directori actualitzat dels certificats expedits i la protecció de la integritat i autenticitat de la informació d'estat de revocació.

L'EC-URV utilitza sistemes fiables per al Dipòsit, de tal manera que:

- Es pugui comprovar l'autenticitat dels certificats.
- Les persones no autoritzades no puguin alterar les dades.
- Els certificats només siguin accessibles en els supòsits o a les persones que el signant indiqui.
- Detecti qualsevol canvi tècnic que afecti els requisits de seguretat.

3. Identificació i autenticació

3.1 Gestió de noms

En aquesta secció s'estableixen requisits relatius als procediments d'identificació i autenticació que s'utilitzen durant el registre dels subscriptors, que s'ha de realitzar amb anterioritat a l'emissió i lliurament de certificats.

3.1.1 Tipus de noms

Tots els certificats contenen un nom diferenciat X.501 en el camp *Subject*, incloent un component *Common Name* (CN=).

3.1.1.1 Característiques dels certificats personals de classe 1 amb càrrec.

Camps	***Valor***
Country	"ES" (correspon al codi ISO de país, corresponent a l'Estat Espanyol).
Organization	El nom de l'Entitat de Registre
Organizational Unit Name	El nom de la Unitat o Departament de l'Entitat de Registre
Organizational Unit Name	El nom del tipus de servei de certificació que es presta
Organizational Unit Name	La direcció web de les condicions generals d'ús del certificat
Surname	Els cognoms del posseïdor de claus, autoritzat per l'Entitat de Registre
Given Name	El nom del posseïdor de claus, autoritzat per l'Entitat de Registre.
Title	La categoria i, opcionalment, el càrrec del posseïdor de claus, separats per un guió, autoritzat per l'Entitat de Registre.
Serial Number	NIF / NIE del posseïdor de claus, autoritzat per l'Entitat de Registre.
Common Name	Un acrònim del servei de certificació i el nom, en text lliure, del posseïdor de claus, autoritzat per l'Entitat de Registre.

El llistat de categories per al camp Title per als certificats personals de classe 1 amb càrrec és el següent:

- "CU " Catedràtics i catedràtiques d'Universitat.
- "TU " Titulars d'universitat
- "CEU" Catedràtics i catedràtiques d'Escoles universitàries
- "TEU" Titulars d'escoles universitàries
- "PRF" Professorat contractat
- "INV" Personal d'investigació
- "PAS" Personal d'Administració i Serveis

3.1.1.2 Característiques dels certificats personals de classe 1 amb càrrec per estrangers.

Camps	***Valor***
Country	"ES" (correspon al codi ISO de país, corresponent a l'Estat Espanyol).
Organization	El nom de l'Entitat de Registre
Organizational Unit Name	El nom de la Unitat o Departament de l'Entitat de Registre
Organizational Unit Name	El nom del tipus de servei de certificació que es presta
Organizational Unit Name	La direcció web de les condicions generals d'ús del certificat
Surname	Els cognoms del posseïdor de claus, autoritzat per l'Entitat de Registre
Given Name	El nom del posseïdor de claus, autoritzat per l'Entitat de Registre.
Title	La categoria i, opcionalment, el càrrec del posseïdor de claus, separats per un guió, autoritzat per l'Entitat de Registre.
Serial Number	Document identificatiu del posseïdor de claus, autoritzat per l'Entitat de Registre, de conformitat amb el punt 3.1.6 de la present DPC.

Camps	*Valor*
Common Name	Un acrònim del servei de certificació i el nom, en text lliure, del posseïdor de claus, autoritzat per l'Entitat de Registre.

El llistat de categories per al camp Title per als certificats personals de classe 1 amb càrrec per estrangers és el següent:

- "EPRF" Professorat estranger
- "EINV" Personal d'investigació estranger

3.1.1.3 Característiques dels certificats personals de classe 2 d'estudiant.

Camps	*Valor*
Country	"ES" (correspon al codi ISO de país, corresponent a l'Estat Espanyol).
Organization	El nom de l'Entitat de Registre
Organizational Unit Name	El nom de la Unitat o Departament de l'Entitat de Registre
Organizational Unit Name	El nom del tipus de servei de certificació que es presta
Organizational Unit Name	La direcció web de les condicions generals d'ús del certificat
Surname	Els cognoms del posseïdor de claus, autoritzat per l'Entitat de Registre
Given Name	El nom del posseïdor de claus, autoritzat per l'Entitat de Registre.
Title	La categoria i, opcionalment, el càrrec del posseïdor de claus, separats per un guió, autoritzat per l'Entitat de Registre.
Serial Number	NIF / NIE del posseïdor de claus, autoritzat per l'Entitat de Registre.
Common Name	Un acrònim del servei de certificació i el nom, en text lliure, del posseïdor de claus, autoritzat per l'Entitat de Registre.

El llistat de categories per al camp Title per als certificats personals de classe 2 és el següent:

- "EST " Estudiants.

3.1.1.4 Característiques dels certificats personals de classe 2 d'estudiant estranger.

Camps	***Valor***
Country	"ES" (correspon al codi ISO de país, corresponent a l'Estat Espanyol).
Organization	El nom de l'Entitat de Registre
Organizational Unit Name	El nom de la Unitat o Departament de l'Entitat de Registre
Organizational Unit Name	El nom del tipus de servei de certificació que es presta
Organizational Unit Name	La direcció web de les condicions generals d'ús del certificat
Surname	Els cognoms del posseïdor de claus, autoritzat per l'Entitat de Registre
Given Name	El nom del posseïdor de claus, autoritzat per l'Entitat de Registre.
Title	La categoria i, opcionalment, el càrrec del posseïdor de claus, separats per un guió, autoritzat per l'Entitat de Registre.
Serial Number	Document identificatiu del posseïdor de claus, autoritzat per l'Entitat de Registre, de conformitat amb el punt 3.1.6 de la present DPC.
Common Name	Un acrònim del servei de certificació i el nom, en text lliure, del posseïdor de claus, autoritzat per l'Entitat de Registre.

El llistat de categories per al camp Title per als certificats personals de classe 2 d'Estudiants estrangers és el següent:

- "EEST" Estudiants Estrangers.

3.1.1.5 Característiques dels certificats d'entitat

Camps	***Valor***
Country	"ES" (correspon al codi ISO de país, corresponent a l'Estat Espanyol).

Camps	*Valor*
Organization	El nom legal del subscriptor (persona jurídica)
Organizational Unit Name	El nom de la Unitat o Departament del responsable
Organizational Unit Name	El nom del tipus de servei de certificació que es presta
Organizational Unit Name	La direcció web de les condicions generals d'ús del certificat
Surname	Els cognoms del responsable de la custodia de claus, autoritzat pel subscriptor
Given Name	El nom del responsable de la custodia de claus, autoritzat pel subscriptor
Serial Number	El Número d'Identificació Fiscal del subscriptor
Common Name	Un acrònim del servei de certificació i la denominació, en text lliure, del subscriptor
1.3.6.1.4.1.18838.1.1	Document identificatiu del responsable de la custodia de claus, autoritzat pel subscriptor, de conformitat amb el punt 3.1.6 de la present DPC

3.1.1.6 Característiques dels CDS

Camps	*Valor*
Country	ES (correspon al codi ISO de país, corresponent a l'Estat Espanyol).
Organization	El nom de l'Entitat de Registre
Organizational Unit Name	El nom de la Unitat o Departament de l'Entitat de Registre
Organizational Unit Name	El nom del tipus de servei de certificació que es presta
Organizational Unit Name	La direcció web de les condicions generals d'ús del certificat

Camps	*Valor*
Common Name	El domini o la adreça IP del servidor

3.1.1.7 Característiques dels CDSCD

Camps	*Valor*
Country	ES (correspon al codi ISO de país, corresponent a l'Estat Espanyol).
Organization	El nom de l'Entitat de Registre
Organizational Unit Name	El nom de la Unitat o Departament de l'Entitat de Registre
Organizational Unit Name	El nom del tipus de servei de certificació que es presta
Organizational Unit Name	La direcció web de les condicions generals d'ús del certificat
Common Name	Adreça IP o DNS del servidor

3.1.1.8 Característiques dels CDA

Camps	*Valor*
Country	ES (correspon al codi ISO de país, corresponent a l'Estat Espanyol).
Organization	El nom de l'Entitat de Registre
Organizational Unit Name	El nom de la Unitat o Departament de l'Entitat de Registre
Organizational Unit Name	El nom del tipus de servei de certificació que es presta
Organizational Unit Name	La direcció web de les condicions generals d'ús del certificat
Serial Number	ID numèric del servidor de l'aplicació
Common Name	ID textual del servidor de l'aplicació

3.1.1.9 Característiques dels CDP

Camps	***Valor***
Country	ES (correspon al codi ISO de país, corresponent a l'Estat Espanyol).
Organization	El nom de l'Entitat de Registre
Organizational Unit Name	El nom de la Unitat o Departament de l'Entitat de Registre
Organizational Unit Name	El nom del tipus de servei de certificació que es presta
Organizational Unit Name	La direcció web de les condicions generals d'ús del certificat
Common Name	El nom del subscriptor – Entitat de Registre – presentació preferida pel subscriptor

3.1.2 Significat dels noms

Als certificats personals la identificació de les persones físiques (posseïdors de claus) està formada pel seu nom i cognoms, més el seu NIF o NIE, o document equivalent, de conformitat amb el punt 3.1.6. La identificació de les persones jurídiques (subscriptors) està formada per la seva denominació o raó social, més el seu CIF.

3.1.3 Utilització d'anònims i pseudònims

No s'utilitzen anònims ni pseudònims en cap cas.

3.1.4 Interpretació de formats de noms

Sense estipulació addicional.

3.1.5 Unicitat dels noms

L'EC-URV emet diferents tipus de certificats. Una mateixa persona (o un mateix posseïdor de claus) només pot disposar d'un únic certificat per a cada tipus de certificats, però pot tenir un certificat d'un altre tipus de certificat de la mateixa EC-URV.

No es pot tornar a assignar un nom de subscriptor que ja hagi estat ocupat, a un subscriptor diferent.

3.1.6 Resolució de conflictes relatius a noms

Els sol·licitants de certificats no poden incloure noms a les sol·licituds que puguin suposar infracció, pel futur subscriptor, de drets de tercers, per exemple emprant documents d'identificació (DNI) falsos.

L'EC-URV no determina que un sol·licitant de certificats té dret sobre el nom que apareix en una sol·licitud de certificat.

Així mateix, no actua com a àrbitre o mitjancer, ni de cap altra manera resol cap disputa concernent a la propietat de noms de persones o organitzacions, noms de domini, marques o noms comercials (per exemple relatius a adreces electròniques).

L'EC-URV es reserva el dret de refusar una sol·licitud de certificat a causa de conflicte de nom.

Els conflictes de noms de posseïdors de claus que apareixen identificats als certificats amb el seu nom real se solucionen mitjançant la inclusió, al nom diferenciat del certificat:

- En cas de nacionals espanyols, el DNI del posseïdor de claus.

  V.gr.: (C) = ES; (SN) = DNI

- En cas d'estrangers, amb algun tipus de vinculació amb Espanya, com pot ser la residència a territori espanyol, el NIE del posseïdor de claus.

  V.gr.: francès (C) = ES; (SN) = NIE

  V.gr.: argentí (C) = ES; (SN) = NIE

- En cas d'estrangers nacionals d'Estats part de l'Acord Schengen i que manquen de NIE, el DNI del país d'origen o de procedència o passaport vigent del posseïdor de claus.

  V.gr.: italià (C) = ES; (SN) = IT-Document nacional d'identitat

- En cas d'estrangers nacionals d'Estats que no són part de l'Acord Schengen i que manquen de NIE, el Passaport ordinari, diplomàtic, oficial o de servei del posseïdor de claus vàlidament expedit i en vigor.

  V.gr.: xinès (C) = ES; (SN) = CN-Passaport

  En els dos supòsits anteriors, junt amb els identificadors esmentats es col·locarà el codi del país del que el posseïdor de claus és nacional, separat per un guió, de conformitat amb els paràmetres establerts per la norma ISO 3166 Codes (Countries).

- Qualsevol altre identificador assignat al posseïdor de claus pel subscriptor.

  V.gr.: un número de carnet URV.

Aquest sistema de resolució de conflictes de noms respon al fet de què la URV, organització subscriptora dels certificats identificada com a tal en el camp "Organizational Unit Name" del "Subject" del perfil dels certificats, està sotmesa a Dret espanyol.

La submissió al Dret espanyol ve determinada per la RFC 3739, la qual estableix que el camp "Subject" contindrà, d'entre altres atributs, l'atribut "countryName" el valor del qual consisteix en especificar el context en el qual s'han d'entendre definits els demés atributs del "Subject", és a dir, en base a la normativa de quin país hem d'entendre semànticament els

demés camps del “Subject”. És, llavors, amb base al “countryName” del “Subject” que s’estableix el significat del “SerialNumber”.

El contingut del “CountryName” del “Subject” s’estableix en atenció a la vinculació més important del subscriptor amb un determinat Estat. Tant en el cas de persones físiques com de persones jurídiques, aquesta vinculació més forta gira, com a norma general, entorn a la seva nacionalitat. Per tant, per determinar el “SerialNumber” del “Subject” s’aplica la normativa reguladora de la nacionalitat i de l’estrangeria d’un determinat Estat, en aquest cas de l’Estat Espanyol.

La identitat dels nacionals espanyols s’acredita amb el Document Nacional d’Identitat o DNI, mentre que la dels estrangers, amb caràcter general, es prova mitjançant el NIE, o Número d’Identificació d’Estrangers, recollit en la Targeta de Identitat d’Estrangers.

Aquells estrangers que manquin de NIE, s’identificaran amb la corresponent documentació acreditativa, la qual variarà en funció de la nacionalitat de l’estranger, diferenciant-se entre els nacionals d’Estats part en l’Acord Schengen y els demés. Els primers acreditaran la seva identitat mitjançant la presentació del seu document nacional de identitat o del seu passaport vàlidament expedit i en vigor. I, els segons, l’acreditaran mitjançant el passaport, el títol de viatge o el document nacional de identitat o cèdula de identificació o qualsevol altre document que acrediti la seva identitat en virtut de compromisos internacionals, en els que quedi perfectament reflectit la identitat i la nacionalitat del titular del document.

En certificats d'entitat, els conflictes de noms dels responsables de la custòdia de claus que apareguin identificats als certificats amb el seu nom real se solucionen mitjançant la inclusió, en el nom diferenciat del certificat, del DNI o NIE del responsable de la custòdia de claus.

Referent al tractament de marques registrades veure l'apartat 9.5.3

3.2 Validació inicial de la identitat

3.2.1 Prova de possessió de clau privada

Aquesta secció descriu els mètodes que s'utilitzen per demostrar que es posseeix la clau privada corresponent a la clau pública objecte de certificació.

El mètode de demostració de possessió de la clau privada és el PKCS #10, una altra prova criptogràfica equivalent o qualsevol mètode aprovat per CATCert.

Aquest requisit no s’aplica quan el parell de claus és generat durant el procés de generació del dispositiu segur de creació de signatura del subscriptor. En aquest supòsit, la possessió de la clau privada es demostra en virtut del procediment fiable de lliurament i acceptació del dispositiu segur i del corresponent certificat i par de claus emmagatzemades al seu interior.

.

3.2.2 Autenticació de la identitat d’una organització

3.2.2.1 La URV

No es requereix realitzar procediment d'autenticació del l’organització subscriptora ja que aquesta i l'Entitat de Registre coincideixen.

3.2.2.2 Altres entitat subscriptores

3.2.2.2.1 Requisits per a certificats de classe 1

No es requereix realitzar procediment d'autenticació de l'organització titular del certificat en certificats de classe 1, ja que es tracta de certificats corporatius, en els quals l'organització subscriptora del certificat i l'Entitat de Registre coincideixen.

3.2.2.2.2 Requisits per a certificats de classe 2

3.2.2.2.2.1 Requisits per a tots els certificats de classe 2

L'Entitat de Certificació ha d'autenticar, amb caràcter previ a l'emissió i lliurament d'un certificat de classe 2 d'organització, la identitat del subscriptor i altres dades, establertes, a la secció corresponent per a certificats d'organització. L'Entitat de Certificació podrà utilitzar Entitats de Registre per a aquesta tasca.

Per tot això, l'Entitat de Certificació o l'Entitat de Registre podran utilitzar els següents mètodes:

1) Obtenció d'informació sobre l'organització, d'un proveïdor extern de serveis d'aquesta naturalesa, a discreció de l'Entitat de Certificació, que prèviament haurà d'aprovar el proveïdor extern.

2) Comprovació de documentació justificativa aportada pel sol·licitant, sobre els següents extrems :

a) Nom legal complet de l'organització

b) Estat legal de l'organització

c) Número d'identificació fiscal

d) Dades d'identificació registral

3.2.2.2.3 Requisits específics per als CDS i els CDSCD

En el cas dels certificats de servidor segur, addicionalment a la comprovació que hagi de fer-se de l'organització responsable del servidor segur, es comprova:

- L'existència del servidor.
- La titularitat del nom de domini provenint del registre corresponent.
- L'autorització per l'organització de l'emissió del certificat al servidor.

3.2.3 Autenticació de la identitat d'una persona física

Aquesta secció conté informacions per a la comprovació de la identitat d'una persona física identificada en un certificat.

3.2.3.1 Elements d'identificació

El número i tipus de documents necessaris per acreditar la identitat del posseïdor de claus són els que admet la URV tal i com es recull en la seva normativa reguladora.

En tot cas, aquests documents identificatius contindran com a mínim:

- Nom i cognoms de la persona
- Lloc i data de naixement
- Número d'identitat reconegut legalment (DNI o NIE)
- Qualsevol altra informació que pugui ser utilitzada per diferenciar una persona de l'altra, dins de l'àmbit de la URV (per exemple: fotografia, correu-e, categoria, càrrec, etc.).

3.2.3.2 Validació dels elements d'identificació

La documentació acreditativa de les dades a certificar (la identitat i demés atributs) es genera mitjançant l'acte administratiu de registre directe per la URV constituïda com Entitat de Certificació Vinculada a l'Entitat de Certificació d'Universitats i Recerca, mitjançant les seves pròpies Entitats de Registre Internes.

Aquesta informació es valida i s'inclou en una base de dades, d'alumnes o de personal de la URV, quan aquest inicia una relació, de caire formatiu, contractual, funcionarial o professional amb la URV.

Aquesta tasca pot ser realitzada per un proveïdor corporatiu d'informació de recursos humans.

Es considera que la informació del posseïdor registrada per la URV en els últims cinc anys està actualitzada.

3.2.3.3 Necessitat de presència personal

És necessari validar la identitat del posseïdor de claus amb la seva presència física, que és responsabilitat de la pròpia URV, i que ho fa mitjançant la seva relació funcionarial, laboral, professional o d'estudiant, segons procedeixi.

Durant el tràmit de lliurament i acceptació del certificat i del corresponent dispositiu segur de creació de signatura, es realitza la validació definitiva de la identitat de la persona de conformitat amb els procediments operatius aprovats i la present DPC.

3.2.3.4 Vinculació de la persona física amb la URV

Com es tracta de certificats corporatius, on l'Entitat de Registre i el subscriptor coincideixen, no és necessari obtenir una justificació documental específica de la vinculació del posseïdor de claus.

3.2.4 Informació de subscriptor no verificada

La URV es responsabilitza que tota la informació inclosa a la sol·licitud del certificat sigui exacta, completa per a la finalitat del certificat. No obstant això no es pot responsabilitzar que es tingui dret al seu ús (per exemple, dret a utilitzar cert nom a l'adreça electrònica o la legitimitat en l'ocupació d'un servidor web).

3.3 Identificació i autenticació de sol·licituds de renovació

3.3.1 Validació per a la renovació rutinària de certificats

S'utilitza el mateix procés que per a l'emissió de certificats.

3.3.2 Validació per a la renovació de certificats després de la revocació

Abans de renovar un certificat - sempre que la causa de la revocació hagi estat diferent del compromís de la clau privada- l'EC-URV comprova que la informació utilitzada per verificar la identitat i les restants dades del subscriptor i del posseïdor de claus continuen sent vàlides.

Si qualsevol informació del subscriptor o del posseïdor de la clau canvia, es registra adequadament la nova informació, d'acord amb l'establert a la secció corresponent.

3.4 Identificació i autenticació de la sol·licitud de revocació

Els titulars dels certificats de la URV estan legitimats per a demanar la revocació dels mateixos però, sempre amb una causa justificada.

Degut a que els certificats pertanyen a una comunitat tancada (la URV) no es considera necessari que es faci cap sol·licitud ni que es signi cap document ja que totes les operacions queden enregistrades.

No obstant això, cal identificar acuradament a la persona compareixent, mitjançant un dels documents d'identitat acceptat a efectes identificatius per la URV.

3.5 Autenticació d'una petició de suspensió

La demanda de suspensió es genera de la mateixa forma que la de revocació o mitjançant el Centre de trucades de CATCert (902 90 10 80) durant les 24 hores del dia, tots els dies de la setmana.

En aquest últim cas, la identificació es realitza mitjançant la verificació, per part de l'operador, de les dades del posseïdor de claus següents: Nom i cognoms, NIF, correu-e, organització, unitat orgànica i número de sèrie del certificat digital que es demana revocar, raó detallada per a la petició de revocació i el codi de suspensió associat al certificat –inclòs en el full de lliurament.

4. Característiques d'operació del cicle de vida dels certificats

4.1 Sol·licitud d'emissió de certificat

4.1.1 Certificats personals

4.1.1.1 Legitimació per a sol·licitar l'emissió

Només pot sol·licitar certificats el sistema d'informació corporatiu de la URV (RRA), mitjançant el corresponent certificat CDA emès per CATCert.

4.1.1.2 Procediment d'alta. Responsabilitats

Diàriament es genera un procés automàtic que revisa les bases de dades, corresponents a alumnes i a personal de la URV, i en detecta les noves incorporacions, així com qualsevol altre modificació de les dades incloses en el certificat, que generarà una nova sol·licitud.

Per cada nova alta a qualsevol de les dues bases de dades anteriorment citades, es genera una sol·licitud de certificat, segons el model establert en manual de procediment operatiu d'emissió de certificats personals, que s'envia per comunicació directa via internet a l'Autoritat de Certificació (AC) de la URV.

La comunicació realitzada a l'AC de la URV es processa i realitzada la validació, si tot és correcte, es crea la sol·licitud a l'Autoritat de Certificació. Seguidament es genera un missatge de resposta informant del resultat positiu o negatiu de la operació i el tipus d'error detectat en cas de resultat negatiu. Aquesta resposta es revisa pel Servei de Recursos Informàtics i TIC, que analitza i canalitza la resolució de les sol·licituds que han estat rebutjades.

4.1.2 Altres certificats

Abans de l'emissió i lliurament d'un certificat, existeix una sol·licitud de certificat, acompanyada de la corresponent documentació acreditativa de les dades a certificar, la qual gestiona el Responsable del Sistema de Certificació Digital de l'URV (en endavant, SCD de l'URV), encarregat de l'Entitat de Registre.

Aquesta sol·licitud només pot ser realitzada pels responsables de les unitats o departaments pertanyents a la comunitat d'usuaris tancada de la URV.

4.2 Processament de la sol·licitud de certificació

4.2.1 Certificats personals

El procediment segueix mitjançant expedients en paper o tramitació electrònica, informàtica o telemàtica, amb la signatura electrònica reconeguda basada en un certificat d'operador emès per CATCert.

L'usuari (professor, membre del PAS o estudiant) es persona físicament a l'Entitat de Registre Interna, amb la seva targeta criptogràfica (carnet URV), prèviament subministrada per Caixa Tarragona, per tal de que l'operador de l'Entitat de Registre Interna verifiqui la seva identitat i comprovi la correcció de les dades carregades al sistema.

Un cop identificat amb l'original del DNI/NIF, NIE, passaport o qualsevol altre document dels admesos conforme a aquesta DPC, insereix la targeta en la unitat de gravació.

Si la sol·licitud és correcta, l'Entitat de Registre Interna:

- Aprova la sol·licitud.
- Imprimeix els codis PIN i PUK que lliura al futur posseïdor de claus
- Genera el certificat dintre de la targeta (carnet URV) del futur posseïdor de claus.
- Fa signar, per duplicat, la documentació de lliurament al posseïdor de claus. En cas que aquest es negui, es revoca el certificat.

Si la petició és incorrecta, perquè alguna de les dades a validar no coincideix exactament amb el document original, es denega la sol·licitud, tot indicant al futur posseïdor de claus la necessitat d'una nova personació, prèvia actualització de les dades existents a la RRA

Si el procediment no es realitza per qualsevol incidència s'emplena un formulari.

4.2.2 Altres certificats

Les sol·licituds realitzades són processades i es realitza la validació. En el supòsit de què tot sigui correcte, es crea la sol·licitud a la EC-URV. Seguidament, es genera un missatge de resposta informant del resultat positiu o negatiu de l'operació i el tipus d'error detectat en cas de ser el resultat negatiu.

4.2.3 Informacions addicionals per al CDS i CDSCD

Una vegada aprovada la sol·licitud de certificat de servidor segur, l'entitat de registre es posa en contacte amb el responsable de la instal·lació del certificat, a fi de determinar el mecanisme de tramesa de la clau pública a certificar.

Després de la recepció, en condicions de seguretat, de la clau pública generada pel sol·licitant, l'EC-URV procedeix a l'emissió del certificat.

4.3 Emissió de certificat

4.3.1 Accions de l'EC-URV durant el procés d'emissió

Nota: Els procediments establerts en aquesta secció també s'apliquen en cas de renovació de certificats, ja que la renovació implica l'emissió d'un nou certificat.

Per a cada sol·licitud de certificat tramitada per l'Entitat de Registre, l'EC-URV:

- Utilitza un procediment de generació de certificats X.509 v3 que vincula de forma segura el certificat amb la informació de registre, incloent la clau pública certificada, mitjançant la signatura digital de l'EC-URV.
- Protegeix la confidencialitat i la integritat de les dades de registre.

- Inclou als certificats personals les informacions establertes a l'article. 11.2 de la Llei 59/2003, d'acord amb l'establert a la secció 3 d'aquest document.
- Compleix les obligacions establertes pels articles 12, 18, 19, 20 i altres aplicables, de la Llei 59/2003, en la generació de certificats reconeguts
- Compleix els controls establerts per aquesta declaració de pràctiques de certificació.

4.3.2 Notificació de l'emissió al subscriptor

L'EC-URV notifica a la URV l'emissió del certificat, o la incidència corresponent.

4.4 Acceptació del certificat

4.4.1 Responsabilitats del Prestador de Serveis de Certificació

4.4.1.1 Per a Certificats personals

El procés que s'efectua conté els següents passos:

- Amb el posseïdor de claus davant l'operador de l'Entitat de Registre Interna i tot seguit d'haver aprovat la sol·licitud de certificat es grava el certificat de forma automàtica a la targeta.
- Es comprova per part de l'operador de l'Entitat de Registre Interna la correcta gravació de tots dos certificats, mitjançant consulta al gestor de la targeta.
- Creació o canvi de dades d'activació de signatura (PIN o contrasenya) pel posseïdor de claus
- Generació tot seguit del full de lliurament del certificat al posseïdor de claus.
- Impressió de dues còpies d'aquest full i signatura del posseïdor d'almenys de la còpia a guardar per l'Entitat de Registre Interna.
- Es lliura l'altra còpia al posseïdor de claus

Al full de lliurament i acceptació del posseïdor, s'indica a aquest:

- quin és el règim obligatori d'ús de certificats digitals:
  - l'existència d'aquesta Declaració de Pràctiques de Certificació,
  - que els certificats són únics per a cada persona i estan protegits per un codi secret,
  - que els certificats permeten identificar-se, generar signatures electròniques i, en el seu cas, desxifrar missatges,
  - que ha de custodiar la targeta i el codi secret,
  - que en cas d'indici que la seva identificació pot ser coneguda per altres persones ha de notificar-ho a la seva Entitat de Registre,
  - Que en cas de necessitat d'informació addicional, pot dirigir-se a la seva Entitat de Registre,

- que pot exercir els seus drets inclosos en la llei 15/1999, de 13 de desembre, sobre protecció de dades personals,
- que les seves dades poden ser cedides, en compliment de la legislació vigent sobre signatura electrònica i protecció de dades personals, i
- quins són els certificats inclosos a la targeta i el codi de suspensió

- que signa el document de lliurament, que hi està d'acord, una vegada llegides i enteses les obligacions i responsabilitats.

4.4.1.2 Per a certificats de dispositiu

S'utilitza el mateix sistema que en l'anterior apartat amb l'única diferència que a la targeta només s'inclou una única clau, corresponent a la clau pública. La clau privada la genera la pròpia entitat que sol·licita el certificat.

4.4.2 Conducta que constitueix acceptació del certificat

El certificat es pot acceptar mitjançant la signatura del full de posseïdor de claus.

4.4.3 Publicació del certificat

Els certificats es poden publicar sense el consentiment previ dels posseïdors de claus, excepte els certificats de classe 2 (d'estudiant) que s'exigeix el previ consentiment dels posseïdors de claus.

4.4.4 Notificació de l'emissió a tercers

No aplicable.

4.5 Ús del parell de claus i del certificat

4.5.1 Ús pels posseïdors de claus

4.5.1.1 Informació per a tots els tipus de certificats

Els certificats s'utilitzen per permetre una millor seguretat en les comunicacions telemàtiques internes de la URV, així com les que es realitzen amb la resta de la societat.

Els certificats s'utilitzen d'acord amb la seva funció pròpia i finalitat establerta, i no es poden utilitzar en altres funcions o amb altres finalitats.

Es té en compte la seva utilització d'acord amb la llei aplicable, tenint en compte les restriccions d'importació i exportació existents en cada moment.

L'ús del parell de claus i del certificat permet al posseïdor de claus identificar-se, generar signatures electròniques i, en el seu cas, desxifrar aquells missatges en els quals l'emissor ha decidit preservar el missatge.

L'extensió Key Usage s'utilitza per establir límits tècnics als usos que pot donar-se a una clau privada corresponent a una clau pública llistada en un certificat X.509v3.

Tanmateix, s'ha de tenir en compte que es dóna la circumstància que l'efectivitat de les limitacions basades en extensions de certificats, depèn en ocasions de l'operació

d'aplicacions informàtiques que no han estat fabricades ni poden estar controlades per l'EC-URV.

4.5.1.2 Informacions específics per als certificats personals i de dispositiu

Els certificats personals i de dispositiu no poden utilitzar-se per signar altres certificats, o informació d'estat de certificats, sota cap circumstància.

4.5.1.3 Informacions addicionals per al CPISR i CESR

Aquests certificats s'utilitzen necessàriament amb un dispositiu segur de creació de signatura electrònica, que compleix les característiques establertes per l'article 24 de la Llei 59/2003, de 19 de desembre i aquesta Declaració de Pràctiques de Certificació (DPC).

S'utilitza el parell de claus exclusivament per crear signatures electròniques i d'acord amb qualsevol altra limitació que sigui notificada.

S'és especialment diligent en la custòdia de la clau privada i del dispositiu segur de creació de signatura, amb la finalitat d'evitar usos no autoritzats.

4.5.1.4 Informacions addicionals per al CPX i CEX

Aquests certificats s'utilitzen en conjunció amb un dispositiu de protecció de la clau privada de desxifrat, d'acord amb les característiques establertes en aquest document.

4.5.2 Ús pel tercer que confia en certificats

Els certificats s'utilitzen d'acord amb la seva funció pròpia i finalitat establerta, sense que puguin utilitzar-se en altres funcions i amb altres finalitats. De la mateixa forma, els certificats s'utilitzen únicament d'acord amb la llei aplicable, especialment tenint en compte les restriccions d'importació i exportació existents en cada moment.

L'ús del certificat permet al tercer que confia, una identificació positiva, rebre i confiar en signatures electròniques i, en el seu cas, xifrar aquells missatges en els quals ha decidit preservar el seu contingut.

L'extensió Key Usage s'utilitza per establir límits tècnics als usos que pot donar-se a una clau privada corresponent a una clau pública llistada en un certificat X.509v3.

Ha de tenir-se en compte que es dóna la circumstància que l'efectivitat de les limitacions basades en extensions de certificats depèn en ocasions de l'operació d'aplicacions informàtiques que no ha estat fabricada ni pot estar controlada per l'EC-URV.

4.6 Renovació de certificats sense renovació de claus

Sense estipulació addicional.

4.7 Renovació de certificats amb renovació de claus

Quan se sol·licita la renovació d'un parell de claus, l'Entitat de Registre Interna verifica que les dades de registre continuen sent vàlides i, si alguna dada ha canviat aquesta és verificada i guardada.

El procediment aplicable a la renovació del certificat és el mateix que per a l'emissió d'un certificat a usuaris nous.

4.8 Modificació de certificats

Sense estipulació addicional.

4.9 Revocació i suspensió de certificats

4.9.1 Causes de revocació de certificats

L'EC-URV pot revocar un certificat per les següents causes:

1. Circumstàncies que afecten la informació continguda al certificat
   - Modificació d'alguna de les dades contingudes al certificat.
   - Descobriment que alguna de les dades contingudes a la sol·licitud de certificat és incorrecta.
   - Descobriment que alguna de les dades contingudes al certificat és incorrecte.
2. Circumstàncies que afecten a la seguretat de la clau o del certificat
   - Compromís de la clau privada o de la infrastructura o sistemes de l'EC-URV, sempre que afecti la confiança en els certificats emesos a partir d'aquest incident.
   - Infracció, per a l'EC-URV, dels requisits previstos en els procediments de gestió de certificats.
   - Compromís o sospita de compromís de la seguretat de la clau o del certificat del subscriptor.
   - Accés o utilització no autoritzat, per un tercer, de la clau privada del subscriptor.
   - L'ús irregular del certificat pel subscriptor o falta de diligència en la custòdia de la clau privada.
3. Circumstàncies que afecten el dispositiu criptogràfic
   - Compromís o sospita de compromís de la seguretat del dispositiu criptogràfic.
   - Pèrdua o inutilització del dispositiu criptogràfic.
   - Accés no autoritzat, per un tercer, a les dades d'activació del subscriptor.
4. Circumstàncies que afecten el subscriptor o el posseïdor de claus
   - Infracció per al sol·licitant del certificat dels requisits preestablerts per a la sol·licitud d'aquest.
   - Infracció per al subscriptor de les seves obligacions, responsabilitat i garanties, establertes a l'instrument jurídic.

- L'extinció de la persona jurídica subscriptora del certificat, així com la finalitat de l'autorització del subscriptor al posseïdor de claus o el final de la relació entre subscriptor i posseïdor de claus.
- Sol·licitud del subscriptor de revocació del certificat, comprovada d'acord amb l'establert a la secció 3.4 d'aquest document.

5. Altres circumstàncies
   - La suspensió del certificat digital per un període superior a 120 dies.
   - El final del servei de l'EC-URV, d'acord amb l'establert a la secció 4.9.1 d'aquest document.

Si l'entitat a la qual es dirigeix la sol·licitud de revocació no disposa de tota la informació necessària per determinar la revocació d'un certificat, però té indicis del seu compromís pot decidir la seva suspensió. En aquest cas es considera que les actuacions realitzades durant el període de suspensió no són vàlides, sempre que el certificat finalment sigui revocat. Seran vàlides si s'aixeca la suspensió i el certificat torna a passar a la situació de vàlid.

La URV ha de sol·licitar la revocació del certificat en cas de tenir coneixement d'alguna de les circumstàncies indicades anteriorment.

4.9.2 Legitimació per a sol·licitar la revocació

1.- El posseïdor de claus del certificat

2.- La URV.

4.9.3 Procediments de sol·licitud de revocació

El procediment de revocació es dur a terme per un dels operadors de l'Entitat de Registre Interna, que accedeix a l'aplicació web, mitjançant un certificat d'operador, de classe 1 o de classe 2, en funció de si és un operador de l'Entitat de Registre o un operador del Centre de Trucades, emès per CATCert, i a continuació i de forma automàtica i immediata s'indica l'esmentada revocació en l'estat del certificat en la llista de revocacions.

L'EC-URV no pot reactivar el certificat, una vegada revocat.

Nota: Un certificat revocat no pot tornar a utilitzar-se; això vol dir que no pot alçar-se la revocació, ni anul·lar-se de cap altra forma: és un estat definitiu del certificat.

4.9.4 Període temporal de sol·licitud de revocació

Les sol·licituds de revocació es remeten de forma raonablement immediata quan es tingui coneixement de la causa de revocació.

4.9.5 Període màxim de processament de la sol·licitud de revocació

La sol·licitud de revocació és processada en el mínim termini possible, sempre dins dels horaris d'oficina de l'EC-URV.

En cas de trobar-se fora d'hores d'oficina, el subscriptor o el posseïdor de claus, ha de sol·licitar la suspensió cautelar del certificat.

4.9.6 Obligació de consulta de informació de revocació de certificats

Els verificadors comproven l'estat d'aquells certificats en què desitgen confiar.

Un mètode pel qual es verifica l'estat dels certificats és consultant la llista de revocació de certificats o LRC més recent emesa per l'EC-URV.

Un altre mètode consisteix en la consulta en línia mitjançant el mecanisme de comprovació d'estat de certificats definit per l'AEAT, en desenvolupament de l'Ordre HAC/1181/2003, de 12 de maig.

L'EC-URV subministra informació als verificadors sobre com i on trobar la LRC corresponent.

4.9.7 Freqüència d'emissió de llistes de revocació de certificats (LRCs)

L'EC-URV emet una LRC almenys cada 24 hores.

S'indica en la LRC el moment programat d'emissió d'una nova LRC, si bé es pot emetre una LRC abans del termini indicat en la LRC anterior.

Els certificats revocats que expirin són retirats de la LRC transcorreguts seixanta dies des de l'expiració.

4.9.8 Període màxim de publicació de LRCs

Les LRCs són publicades immediatament en el Registre de certificació de l'EC-URV.

4.9.9 Disponibilitat de serveis de comprovació d'estat de certificats

Els serveis de comprovació d'estat de certificats es troben disponibles 24 hores al dia, 7 dies per setmana.

4.9.10 Obligació de consulta de serveis de comprovació d'estat de certificats

El verificador que no utilitza LRC per comprovar la validesa d'un certificat, ho pot fer en el Dipòsit de l'EC-URV.

Els verificadors han de comprovar obligatòriament l'estat d'aquells certificats en què desitgen confiar.

Una forma per la qual es verifica l'estat dels certificats és consultant la LRC més recent de l'EC-URV.

L'EC-URV subministra informació als verificadors referent a com i on trobar la LRC corresponent.

4.9.11 Altres formes d'informació de revocació de certificats

L'EC-URV pot establir altres formes per informar sobre la revocació dels certificats, com per exemple el mecanisme de comprovació d'estat de certificats definit per l'AEAT, en desenvolupament de l'Ordre HAC/1181/2003, de 12 de maig.

4.9.12 Procediments especials en cas de compromís de la clau privada

El compromís de la clau privada de l'EC-URV és notificat, en la mesura possible, a tots els participants en la jerarquia pública de certificació de Catalunya i a tots els tercers verificadors, mitjançant el Registre de Certificació de CATCert.

4.9.13 Causes de suspensió de certificats

Els certificats es poden suspendre:

- Quan ho sol·liciti el posseïdor de claus o el subscriptor
- Quan la documentació requerida a la sol·licitud de revocació sigui suficient però no es pugui identificar raonablement el posseïdor de claus.
- Quan la documentació requerida a la sol·licitud de revocació no sigui suficient, encara que es pugui identificar raonablement el posseïdor de claus
- Quan la documentació requerida a la sol·licitud de revocació no sigui suficient i tampoc no permetin identificar raonablement el posseïdor de claus.
- Si el subscriptor no utilitza el certificat durant un període prolongat de temps, conegut prèviament
- Si se sospita el compromís d'una clau, fins que aquest sigui confirmat. En aquest cas, l'EC-URV ha d'assegurar-se que el certificat no està suspès durant més temps del necessari per consignar el seu compromís.
- Quan no s'activa el certificat en un termini de 120 dies a partir de la data d'emissió del certificat.

4.9.14 Qui pot sol·licitar la suspensió

1. El posseïdor de claus del certificat
2. La URV.

4.9.15 Procediments de petició de suspensió

El procediment de suspensió, es genera de la mateixa forma que el procediment de revocació i, es dur a terme per un dels operadors de l'Entitat de Registre Interna, que accedeix a l'aplicació web, mitjançant un certificat d'operador, de classe 1 o de classe 2, segons sigui operador de la URV o del Centre de Trucades, respectivament.

La suspensió dels certificat digitals es pot realitzar de les formes que es detallen a continuació:

1. La suspensió pot ser sol·licitada pels subjectes legitimats per mitjà d'una trucada al 902 90 10 80 (Centre de trucades de CATCert).
2. La suspensió pot ser realitzada per l'Entitat de Registre Interna directament, a través del component LRA o RRA.
3. La suspensió pot ser realitzada per l'EC-URV directament, a través del component LRA o RRA.

4.9.16 Període màxim de suspensió

El termini màxim de suspensió serà de cent vint dies naturals.

4.10 Serveis de comprovació d'estat de certificats

4.10.1 Característiques d'operació dels serveis

Les LRC són descarregades manualment des del Dipòsit de Certificació de CATCert instal·lades per als verificadors.

4.10.2 Disponibilitat dels serveis

Els sistemes de distribució de LRCs i de consulta en línia de l'estat dels certificats estan disponibles les 24 hores dels 7 dies de la setmana.

En cas d'error dels sistemes de comprovació d'estat de certificats per causes fora del control de l'EC-URV, aquesta realitza els seus millors esforços per assegurar que aquest servei es manté inactiu el mínim temps possible. L'EC-URV detalla en l'apartat 5.7.4 d'aquest document el màxim temps en què el servei ha de tornar a operar.

L'EC-URV subministra informació als verificadors sobre el funcionament del servei d'informació d'estat de certificats.

4.10.3 Altres funcions dels serveis

Sense estipulació addicional.

4.11 Acabament de la subscripció

L'acabament de la subscripció no implica la revocació dels certificats que hagin estat emesos, sinó que aquests poden utilitzar-se fins que expirin.

4.12 Dipòsit i recuperació de claus

4.12.1 Política i pràctiques de dipòsit i recuperació de claus

La recuperació de claus la realitza CATCert.

4.12.2 Política i pràctiques d'encapçalament i recuperació de claus de sessió

Sense estipulació addicional.

5. Controls de seguretat física, de gestió i d'operacions

L'EC-URV i les Entitats de Registre s'asseguren de l'aplicació dels procediments administratius i de gestió adequats i conformes amb els estàndards reconeguts i, en particular:

a. Es realitza un anàlisi de gestió de risc per avaluar les necessàries mesures de seguretat.

b. S'és responsable per la provisió dels serveis de forma segura, fins i tot quan una part dels mateixos sigui subcontractada. Les responsabilitats dels tercers són definides i cal implantar els necessaris controls jurídics per garantir que els tercers compleixen les seves obligacions amb un nivell equivalent de seguretat.

c. S'estableixen les normes principals en matèria de seguretat mitjançant un òrgan d'alt nivell que defineix la política de seguretat de la informació de l'Entitat, i dona la necessària publicitat mitjançant accions de comunicació interna.

d. Es manté en tot moment la infraestructura necessària per gestionar la seguretat de les operacions. Qualsevol canvi que tingui impacte en el nivell de seguretat ha de ser aprovat per l'òrgan referit al número anterior.

e. Es documenten, s'implanten i es mantenen els controls de seguretat i procediments d'operació de les instal·lacions, sistemes i actius d'informació en què es sustenta la prestació dels serveis.

En cas de subcontractació total dels serveis, es garanteix que es manté el necessari nivell de seguretat de la informació.

5.1 Controls de seguretat física

L'EC-URV disposa d'instal·lacions que protegeixen físicament la prestació, almenys, dels serveis de generació de certificats, de dispositius criptogràfics i de gestió de revocació, del compromís causat per accés no autoritzat als sistemes o a les dades.

Igualment, les Entitats de Registre que generin certificats dins de dispositius segurs de creació de signatura o d'altres mòduls de seguretat criptogràfica també disposen d'equivalents mesures de seguretat física, que són aprovades per l'EC-URV i per CATCert.

La protecció física s'aconsegueix mitjançant la creació de perímetres de seguretat clarament definits entorn dels serveis de generació de certificats, de dispositius criptogràfics i de gestió de revocació. La part de les instal·lacions compartides amb altres organitzacions es troba fora d'aquests perímetres.

L'EC-URV i les Entitats de Registre estableixen controls de seguretat física i ambientals per protegir els recursos de les instal·lacions on es troben els sistemes, els mateixos sistemes i els equipaments utilitzats per a les operacions. La política de seguretat física i ambiental aplicable als serveis de generació de certificats, de dispositius criptogràfics i de gestió de revocació estableix prescripcions per a les següents contingències:

- Controls d'accés físic
- Protecció davant de desastres naturals
- Mesures de protecció davant d'incendis
- Error dels sistemes de suport (energia elèctrica, telecomunicacions, etc.)
- Demolició de l'estructura
- Inundacions
- Protecció antirobatoris
- Conformitat i entrada no autoritzada
- Recuperació del desastre
- Sortida no autoritzada d'equipaments, informacions, suports i aplicacions relatius a components utilitzats per als serveis de l'EC-URV.

Aquesta política de seguretat física i ambiental és revisada i aprovada pel Consell de Govern de l'URV i, definitivament, per CATCert, abans d'iniciar les operacions de l'Entitat de Certificació o de Registre.

5.1.1 Localització i construcció de les instal·lacions

La localització de les instal·lacions permet la presència de forces de seguretat en un termini de temps raonablement immediat des que una incidència els sigui notificada (en el cas de no comptar amb presència física permanent de personal de seguretat de l'EC-URV).

La qualitat i solidesa dels materials de construcció de les instal·lacions garanteix uns adequats nivells de protecció davant d'intrusions per força bruta.

Quan l'Entitat de Registre Interna realitza serveis de preparació, inicialització i gestió de dispositius criptogràfics sense la presència física del seu posseïdor de claus (professor, PAS o estudiant), ha de disposar d'un entorn físicament protegit i diferent, sota la responsabilitat del departament responsable de les tasques de registre, i no poden estar compartides amb cap altre departament, organització o empresa.

5.1.2 Accés físic

L'EC-URV estableix nivells de seguretat amb restricció d'accés als diferents perímetres i barreres físiques definides.

Per a l'accés a les dependències de l'EC-URV on es duguin a terme processos relacionats amb el cicle de vida del certificat, és necessària l'autorització prèvia", identificació en el moment de l'accés i registre del mateix, incloent filmació per circuit tancat de televisió i el seu arxiu.

Aquesta identificació, davant del sistema de control d'accessos, es realitza mitjançant reconeixement d'algun paràmetre biomètric de l'individu, excepte en cas de visites escortades.

Per l'accés a les dependències de les Entitats de Registre cal utilitzar una contrasenya segura de l'individu, excepte en cas de visites escortades.

La generació de claus criptogràfiques de l'EC-URV, així com el seu emmagatzematge, es realitza en dependències específiques per a aquestes finalitats, i requereixen d'accés i permanència dobles.

Quan l'Entitat de Registre Interna realitza serveis de preparació, inicialització i gestió de dispositius criptogràfics sense la presència física del seu posseïdor de claus (professor, PAS o estudiant), es tenen en consideració les següents mesures de control d'accés físic:

- Està restringit l'accés al públic en general
- L'accés roman tancat quan no hi hagi cap responsable de l'Entitat de Registre
- Només els responsables de l'Entitat de Registre disposen de clau
- En cas de molta afluència de públic, es preveu l'assistència de personal de seguretat

5.1.3 Electricitat i aire condicionat

Els equips informàtics de l'EC-URV estan convenientment protegits davant de fluctuacions o talls de subministrament elèctric, que puguin danyar-los o interrompin el servei.

Les instal·lacions compten amb un sistema d'estabilització del corrent, així com d'un sistema de generació propi amb autonomia suficient per mantenir el subministrament durant el temps que requereixi el tancament ordenat i complet de tots els sistemes informàtics".

Els equips informàtics estan ubicats en un entorn on es garanteix una climatització (temperatura i humitat) adequada a les seves condicions òptimes de treball.

5.1.4 Exposició a l'aigua

L'EC-URV disposa de sistemes de detecció d'inundacions adequats per protegir els equips i actius davant d'aquesta eventualitat, en el cas, que les condicions d'ubicació de les instal·lacions ho fessin necessari.

5.1.5 Advertència i protecció d'incendis

Totes les instal·lacions i actius de l'EC-URV compten amb sistemes automàtics de detecció i extinció d'incendis.

En concret, els dispositius criptogràfics, i suports que emmagatzemen claus de l'EC-URV, compten amb un sistema específic i addicional a la resta de la instal·lació, per a la protecció davant del foc.

5.1.6 Emmagatzematge de suports

L'emmagatzematge en suports d'informació es realitza de manera que es garanteixi tant la seva integritat com la seva confidencialitat, d'acord amb la classificació de la informació que s'hagi establert.

Les còpies es guarden en format CD, i aquests en caixa forta a la mateixa sala.

L'accés a aquests suports, fins i tot per a la seva eliminació, està restringit a persones específicament autoritzades.

Tenim en compte que les entitats de registre es queden amb una còpia signada pel posseïdor de claus del full de lliurament de certificats. Aquesta còpia es guardada durant 15

anys per l'Entitat de Registre, aplicant-li allò que indica la legislació catalana d'arxius, en relació amb la guarda i custòdia de documentació.

5.1.7 Tractament de residus

L'eliminació de suports, tant paper com de magnètics, es realitza mitjançant mecanismes que garanteixen la impossibilitat de recuperació de la informació.

En el cas de suports magnètics, es procedeix al formatatge, esborrament permanent, o destrucció física del suport.

En el cas de documentació en paper, aquest se sotmet a un tractament físic de destrucció.

5.1.8 Còpia de seguretat fora de les instal·lacions

Periòdicament, l'EC-URV emmagatzema un backup dels sistemes d'informació, en dependències físicament separades d'aquelles en les quals es troben els equips.

En el moment de realitzar una sortida d'informació de les dependències hem d'adoptar mesures adients per a impedir qualsevol recuperació indeguda de l'esmentada informació (com per exemple la utilització de carteres amb dispositius segurs de claus o combinacions, o la utilització de fitxers encriptats)

5.2 Controls de procediments

L'EC-URV garanteix que els seus sistemes s'operen de forma segura, i per això estableix i implanta procediments per a les funcions que afecten la provisió dels seus serveis.

El personal al servei de l'EC-URV realitza els procediments administratius i de gestió d'acord amb la política de seguretat de l'EC-URV. Aquesta política de seguretat ofereix suport a rols amb diferents privilegis.

5.2.1 Funcions fiables

Les persones que ocupen aquests llocs són formalment nomenades per l'alta direcció de l'EC-URV.

Les funcions fiables inclouen:

- Oficial de seguretat.
- Operador de registre.
- Administradors del sistema
- Operadors del sistema
- Auditors del sistema
- Qualsevol altra persona amb accés a dades de caràcter personal

Les funcions i obligacions fiables es defineixen a la secció 5.3 d'aquest document.

5.2.2 Nombre de persones per tasca

Les funcions fiables identificades en la política de seguretat de l'EC-URV, i les seves responsabilitats associades, estan documentades en descripcions de llocs de treball.

5.2.3 Identificació i autenticació per a cada funció

L'EC-URV identifica i autentica el personal abans d'accedir a la corresponent funció fiable.

5.2.4 Rols que requereixen separació de tasques

L'EC-URV identifica, en la seva política de seguretat, funcions o rols fiables.

Les següents restriccions s'apliquen en tot cas:

a. La persona que actua com oficial de seguretat o com operador de registre no pot ser auditor del sistema.

b. La persona que actua com administrador del sistema no pot ser oficial de seguretat ni auditor del sistema.

c. Quan el registre es practicat per una Entitat de Registre Interna en presència personal del posseïdor de claus, l'oficial de registre pot aprovar i generar el certificat, mentre que en la resta de casos, i especialment quan el registre es practica de forma delegada per una Entitat de Registre Col·laboradora, serà imprescindible segregar els rols d'aprovador i generador (gaudint tots dos de la consideració d'operadors de registre).

Les esmentades descripcions es realitzen tenint en compte que existeix una separació de funcions sensibles, així com una concessió de mínim privilegi, quan sigui possible. Per determinar la sensibilitat de la funció, es tenen en compte els següents elements:

a. Deures associats a la funció

b. Nivell d'accés

c. Monitoratge de la funció

d. Formació i conscienciació

e. Habilitats requerides

5.3 Controls de personal

L'EC-URV té en compte els següents aspectes:

- Es manté confidencialitat de la informació, posant els mitjans necessaris i mantenint una actitud adequada en el desenvolupament de les seves funcions i, fora de l'àmbit laboral en allò referent a la seguretat de les infrastructures.

- S'és diligent i responsable en el tractament, manteniment i custòdia dels actius de la infrastructura identificats en la política, en els plans de seguretat o en aquest document.

- No es revela informació no pública fora de l'àmbit de la infrastructura, ni s'extreuen suports d'informació a nivells de seguretat inferiors.

- Es reporta al Responsable de Seguretat, el més aviat possible, qualsevol incident que es consideri que afecta a la seguretat de la infrastructura, o limitar la qualitat del servei.

- S'utilitzen els actius de la infrastructura per a les finalitats que els han estat encomanades.

- S'exigeixen manuals o guies d'usuari dels sistemes que utilitza, que permeten desenvolupar la seva funció correctament.

- S'exigeix documentació escrita que marqui les seves funcions i mesures de seguretat a què està sotmès.

- El responsable de seguretat vetlla perquè el punt anterior sigui executat, proveint els responsables d'àrea tota la informació que fos necessària.

- No s'instal·len en cap dels sistemes de la infrastructura, programari o maquinari que no sigui expressament autoritzat per escrit pel responsable de sistemes d'informació.

- No s'accedeix voluntàriament, ni no s'elimina o altera informació no destinada a la seva persona o perfil professional.

El personal afectat per aquesta normativa és:

- el Responsable del Servei
- el Responsable de l'EC-URV
- el Responsable de Seguretat
- el Responsable d'Operacions
- l'Operador de Cerimònies de Claus
- l'Equip tècnic d'administració, operació i explotació
- els Administradors de la Xarxa
- i els Usuaris de les Entitats de Registre.

5.3.1 Requisits d'historial, qualificacions, experiència i autorització

L'EC-URV ocupa personal qualificat i amb l'experiència necessària per a la prestació dels serveis oferts, en l'àmbit de la signatura electrònica i els procediments de seguretat i de gestió adequats.

Aquest requisit s'aplicarà al personal de gestió de l'EC-URV, especialment en relació amb procediments de personal de seguretat.

La qualificació i l'experiència poden suplir-se mitjançant una formació i entrenament apropiats.

El personal en llocs fiables es troba lliure d'interessos personals que entrin en conflicte amb el desenvolupament de la funció que tingui encomanada.

L'EC-URV no assigna a un lloc fiable o de gestió una persona que no sigui idònia per al lloc, especialment per haver estat condemnada per delicte o falta que afecti la seva idoneïtat per al lloc. Per aquest motiu, l'EC-URV realitza una investigació relativa als següents aspectes:

- Antecedents penals

- Estudis, incloent titulació al·legada
- Treballs anteriors, fins cinc anys, incloent referències professionals i comprovació que realment es va realitzar el treball al·legat
- Morositat

5.3.2 Procediments d'investigació d'historial

L'EC-URV realitza la investigació abans que la persona sigui contractada i accedeixi al lloc de treball.

A la sol·licitud per al lloc de treball s'informa sobre la necessitat de sotmetre's a una investigació prèvia.

S'adverteix que la negativa a sotmetre's a la investigació implica el rebuig de la sol·licitud.

L'EC-URV obté consentiment inequívoc de l'afectat per a la investigació prèvia i processa i protegeix totes les seves dades personals d'acord amb la LOPD i el Reglament de Mesures de Seguretat de la LORTAD.

La investigació al personal contractat es repeteix cada tres anys.

El personal de la URV garanteix un nivell de confiança i qualificació adequats per realitzar les tasques assignades.

L'Entitat de Registre Interna està assabentada que cap candidat no té interessos que interfereixin amb les seves futures funcions, així com que no ha estat condemnat per algun delicte que alteri la seva idoneïtat per a aquesta tasca.

5.3.3 Requisits de formació

L'EC-URV forma el personal en llocs fiables i de gestió, fins que aconsegueixen la qualificació necessària.

La formació inclou els següents continguts:

- Principis i mecanismes de seguretat de la jerarquia pública de certificació de Catalunya, així com l'entorn d'usuari de la persona a formar.
- Versions de maquinari i aplicacions en ús
- Tasques que realitza la persona
- Gestió i tramitació d'incidents i compromisos de seguretat
- Procediments de continuïtat de negoci i emergència
- Procediment de gestió i de seguretat en relació amb el tractament de les dades de caràcter personal

La URV (o les Entitats de Registre Internes quan pertoqui), a més, proporciona tot el personal involucrat en les operacions de l'Entitat de Registre, una informació adequada, que inclou els procediments de treball i els de seguretat. També es realitza instrucció periòdica en normes de seguretat, plans de contingència i gestió d'incidències.

5.3.4 Requisits i freqüència d'actualització formativa

Tot el personal vinculat a l'Entitat de Registre té com a requisit imprescindible l'assistència al curs de formació d'Entitats de Registre donat per CATCert.

5.3.5 Seqüència i freqüència de rotació laboral

Sense estipulació addicional.

5.3.6 Sancions per accions no autoritzades

L'EC-URV disposa d'un sistema sancionador, que depura les responsabilitats derivades d'accions no autoritzades.

Les accions disciplinàries inclouen la suspensió i l'acomiadament de la persona responsable de l'acció danyosa.

5.3.7 Requisits de contractació de professionals

L'EC-URV contracta professionals per a qualsevol funció, fins i tot per a un lloc fiable, cas en el qual se sotmet als mateixos controls que els empleats restants.

En el cas que el professional no hagi de sotmetre's a aquests controls, està constantment acompanyat per un empleat fiable.

En el cas que tots o una part dels serveis de certificació siguin operats per un tercer, els controls i previsions realitzats en aquesta secció 5, o en altres parts de la política de certificat o de la DPC, són aplicats i completats pel tercer que realitza les funcions d'operació dels serveis de certificació, l'EC-URV és responsable en tot cas de l'efectiva execució.

Aquests aspectes queden concretats a l'instrument jurídic utilitzat per acordar la prestació dels serveis de certificació pel tercer diferent de l'EC-URV.

5.3.8 Subministrament de documentació al personal

L'EC-URV subministra la documentació que estrictament necessita el seu personal en cada moment, amb la finalitat que sigui prou competent.

5.4 Procediments d'auditoria de seguretat

5.4.1 Tipus d'esdeveniments registrats

L'EC-URV guarda registre, com a mínim, dels següents esdeveniments relacionats amb la seguretat de l'entitat:

- Encès i apagat dels sistemes
- Inici i acabament de l'aplicació d'Autoritat (tècnica) de certificació
- Intents de crear, esborrar, canviar contrasenyes o permisos dels usuaris dins del sistema
- Canvis en les claus de l'Autoritat (tècnica) de certificat
- Canvis en les polítiques d'emissió de certificats

- Intents d'entrada i sortida del sistema
- Intents no autoritzats d'entrada a la xarxa de l'EC-URV
- Intents no autoritzats d'accés als fitxers del sistema
- Generació de les claus de l'EC-URV
- Intents nuls de lectura i escriptura en un certificat i en el Dipòsit
- Esdeveniments relacionats amb el cicle de vida del certificat, com una sol·licitud, emissió, revocació i renovació d'un certificat
- Esdeveniments relacionats amb el cicle de vida del mòdul criptogràfic, com a recepció, ús i desinstal·lació d'aquest.

L'EC-URV també guarda, ja sigui manualment o electrònicament, la següent informació:

- La cerimònia de generació de claus i les bases de dades de gestió de claus
- Registres d'accés físic
- Manteniments i canvis de configuració del sistema
- Canvis en el personal
- Informes de compromisos i discrepàncies
- Registres de la destrucció de material que contingui informació de claus, dades d'activació o informació personal del subscriptor.
- Possessió de dades d'activació, per a operacions amb la clau privada de l'EC-URV
- Informes complets dels intents d'intrusió física en les infraestructures que donen suport a l'emissió i gestió de certificats.

5.4.2 Freqüència de tractament de registres d'auditoria

Els registres d'auditoria s'examinen almenys una vegada al mes a la recerca d'activitat sospitosa o no habitual

El processament dels registres d'auditoria consisteix en una revisió dels registres que inclou la verificació que aquests no han estat manipulats, una breu inspecció de totes les entrades de registre i una investigació més profunda de qualsevol alerta o irregularitat en els registres. Les accions realitzades a partir de la revisió d'auditoria també estan documentades.

5.4.3 Període de conservació de registres d'auditoria

Els registres d'auditoria es retenen durant almenys dos mesos després de processar-los i a partir d'aquell moment s'arxiven d'acord amb la secció 5.5 d'aquest document.

5.4.4 Protecció dels registres d'auditoria

Els fitxers de registre, tant manuals com electrònics, es protegeixen de lectures, modificacions, esborraments o qualsevol altre tipus de manipulació no autoritzada usant controls d'accés lògic i físic.

5.4.5 Procediments de còpies de seguretat

Es generen còpies de suport incrementals de registre d'auditoria diàriament i còpies completes setmanalment.

Per tal de conservar correctament les còpies de seguretat s'han implantat els següents punts:

- Es guarden en armaris ignífugs
- Només persones autoritzades disposen d'accés a les còpies de seguretat.
- Les còpies estan identificades
- Si un material ha contingut còpies de seguretat (disquets, dvd's...) i es vol reutilitzar ens assegurem que les dades que ha contingut han estat totalment esborrades fent impossible la seva recuperació
- S'autoritza expressament l'extracció de les còpies fora de l'Entitat de Registre, emplenant una fitxa al respecte i anotant el corresponent detall en un llibre de registre.
- Es té cura d'anar dipositant còpies de seguretat periòdicament fora de l'Entitat de Registre.

5.4.6 Localització del sistema d'acumulació de registres d'auditoria

El sistema d'acumulació de registres d'auditoria és, almenys, un sistema intern de l'EC-URV, compost pels registres de l'aplicació, pels registres de xarxa i pels registres del sistema operatiu, a més de per les dades manualment generades, que seran emmagatzemades pel personal degudament autoritzat.

5.4.7 Notificació de l'esdeveniment d'auditoria al causant de l'esdeveniment

Quan el sistema d'acumulació de registres d'auditoria registra un esdeveniment, no és necessari enviar una notificació a l'individu, organització, dispositiu o aplicació que va causar l'esdeveniment.

Es comunica si el resultat de la seva acció ha tingut èxit o no, però no que s'ha auditat l'acció.

5.4.8 Anàlisis de vulnerabilitats

Els esdeveniments en el procés d'auditoria són guardats, en part, per monitoritzar les vulnerabilitats del sistema.

Les anàlisi de vulnerabilitat són executades, repassades i revisades per mitjà d'un examen d'aquests esdeveniments monitoritzats

Aquestes anàlisis són executades diàriament, mensualment i anualment d'acord amb la seva definició en el Pla d'Auditoria de l'EC-URV.

5.5 Arxiu d'informacions

L'EC-URV garanteix que tota la informació relativa als certificats es guarda durant un període de temps apropiat, segons el que s'estableix a la secció 5.5.2, i que es gestiona de conformitat amb el procediment d'arxiu aprovat.

5.5.1 Tipus d'esdeveniments registrats

L'EC-URV guarda tots els esdeveniments que tinguin lloc durant el cicle de vida d'un certificat, incloent la renovació d'aquest.

L'EC-URV guarda un registre del següent:

Documents originals:

- Formulari de sol·licitud de certificats
- Certificat de dades
- Full de lliurament de subscriptor de certificats

Fotocòpies de:

- Carta de lliurament de certificats CPISR i CPX
- Carta PIN i PUK, amb justificant de recepció.

5.5.2 Període de conservació de registres

L'EC-URV guarda els registres especificats a la secció 5.5.1. durant 15 anys, comptats des del moment de l'expedició del certificat.

5.5.3 Protecció de l'arxiu

L'EC-URV:

- Manté la integritat i la confidencialitat de l'arxiu que conté les dades referents als certificats emesos.
- Arxiva les dades indicades anteriorment de forma completa i confidencial.
- Manté la privacitat de les dades de registre del subscriptor.

5.5.4 Procediments de còpia de suport

Es fan còpies de seguretat dels logs d'accés lògic al sistema operatiu de la LRA.

Aquestes còpies de seguretat es realitzen amb una periodicitat mensual i es guarden en format CD, i aquests discs en una caixa forta present a la mateixa sala.

Es realitzen també còpies de seguretat de l'aplicació KeyOne personalitzada per a la URV. Aquestes còpies les guarda CATCert a les seves instal·lacions.

5.5.5 Requisits de segellat de cautela de data i hora

L'EC-URV emet els certificats i les LRC amb informació de temps i hora. No és necessari que aquesta informació es trobi signada.

5.5.6 Localització del sistema d'arxiu

L'EC-URV té un sistema de manteniment de dades d'arxiu fora de les seves pròpies instal·lacions, així com s'especifica a la secció 5.1.8.

5.5.7 Procediments d'obtenció i verificació d'informació d'arxiu

Només persones autoritzades per l'EC-URV tenen accés a les dades d'arxiu, sigui a les mateixes instal·lacions de l'EC-URV o en la seva ubicació externa.

5.6 Renovació de claus

Els certificats de l'EC-URV renovats es comuniquen als usuaris finals, mitjançant la seva publicació en el Registre de CATCert.

5.7 Compromís de claus i recuperació de desastre

5.7.1 Procediment de gestió d'incidències i compromisos

L'EC-URV estableix els procediments que aplica en la gestió de les incidències que afecten les seves claus i, molt especialment, en els compromisos de la seguretat de les claus.

5.7.2 Corrupció de recursos, aplicacions o dades

Quan tingui lloc un esdeveniment de corrupció de recursos, aplicacions o dades l'EC-URV inicia les gestions necessàries, segons els documents Pla de Seguretat, Pla d'Emergència i Pla d'Auditoria, per fer que el sistema torni al seu estat normal de funcionament.

5.7.3 Compromís de la clau privada de l'EC-URV

El pla de continuïtat de negoci de l'EC-URV (o pla de recuperació de desastres) considera el compromís o la sospita de compromís de la clau privada de l'EC-URV com un desastre.

En cas de compromís l'EC-URV:

- Informa a tots els subscriptors i verificadors del compromís.
- Indica que els certificats i la informació de l'estat de revocació lliurats usant la clau de l'EC-URV ja no són vàlids.

5.7.4 Desastre sobre les instal·lacions

L'EC-URV desenvolupa, manté, testa i, si és necessari, executa un pla d'emergència en el cas de desastre, ja sigui per causes naturals o causat per l'home, sobre les instal·lacions, que indica com es restauren els serveis dels Sistemes d'Informació. La ubicació dels sistemes de recuperació de desastre disposa de les proteccions físiques de seguretat detallades en el Pla de Seguretat.

L'EC-URV és capaç de restaurar l'operació normal de la PKI en les 24 hores següents al desastre, podent executar-se, com a mínim, les següents accions:

- Revocació de certificats (excepte el mes d'agost)

- Publicació d'informació de revocació

La base de dades de recuperació de desastres utilitzada per l'EC-URV està sincronitzada amb la base de dades de producció, dins dels límits temporals especificats en el Pla de Seguretat. Els equips de recuperació de desastres de l'EC-URV tenen les mesures de seguretat físiques especificades en el Pla de Seguretat.

5.8 Acabament del servei

5.8.1 EC-URV

L'EC-URV assegura que les possibles interrupcions als subscriptors i a terceres parts són mínimes com a conseqüència del cessament dels serveis de l'EC-URV i, en particular, assegura un manteniment continu dels registres requerits per proporcionar evidència de certificació en procediments legals.

Abans d'acabar els seus serveis l'EC-URV executa, com a mínim, els següents procediments:

- Informa a tots els subscriptors i verificadors (no es requereix que l'EC-URV tingui alguna relació anterior amb terceres parts).
- Acaba tota autorització de subcontractacions que actuïn en nom de l'EC-URV en el procés d'emissió de certificats.
- Executa les tasques necessàries per transferir les obligacions de manteniment de la informació de registre i els arxius de registre d'esdeveniments durant els períodes de temps respectius indicats al subscriptor i als verificadors.
- Destrueix les claus privades de l'EC-URV o les retira de l'ús.

L'EC-URV declara en les seves pràctiques les previsions que té per al cas d'acabament del servei. Aquestes inclouen:

- Notificació a les entitats afectades
- Transferència de les obligacions de l'EC-URV a altres persones
- Com es tracta l'estat de revocació dels certificats emesos que encara no han expirat.

L'EC-URV transfereix els certificats, en els termes previstos en la Llei 59/2003, de 19 de desembre.

5.8.2 Entitat de Registre

Sense estipulació addicional.

6. Controls de seguretat tècnica

L'EC-URV utilitza sistemes i productes fiables, que estan protegits contra tota alteració i que garanteixen la seguretat tècnica i criptogràfica dels processos de certificació als que serveixen de suport.

6.1 Generació i instal·lació del parell de claus

6.1.1 Generació del parell de claus

6.1.1.1 Informació per als certificats CPISR i CESR

Les claus pública i privada dels certificats CPISR i CESR es generen sota la seva responsabilitat, per part de l'Entitat de Registre dins d'un dispositiu segur de creació de signatura electrònica (targeta que rep el posseïdor de claus)

6.1.1.2 Informació per als certificats CPX i CEX

Les claus pública i privada dels certificats CPX i CEX es generen sota la seva responsabilitat, per part de l'Entitat de Registre i són inserides al dispositiu de desxifrat.

Addicionalment una còpia de la clau privada s'emmagatzema a l'Entitat de Registre, excepte quan el subscriptor no desitja aquest servei.

6.1.1.3 Informació per als certificats CDS i CDSCD

La clau pública dels certificats CDS i CDSCD es genera sota la seva responsabilitat, per part de l'Entitat de Registre dins d'un dispositiu segur de creació de signatura electrònica. La clau privada la genera la URV que sol·licita el certificat, i en cap cas s'envia a l'Entitat de Registre Interna.

Els certificats de dispositiu de servidor segur s'emeten a les facultats i centres universitaris de la URV, responsables de l'operació de servidors segurs per als següents usos:

- Autenticació de servidor
- Xifrat de les comunicacions entre client i servidor

6.1.2 Enviament de la clau privada al subscriptor

La clau privada del subscriptor, li és lliurada degudament protegida mitjançant una targeta intel·ligent que compleix els requisits establerts per les especificacions tècniques CEN CWA 14169 i CWA 14170 o equivalent.

6.1.3 Enviament de la clau pública a l'emissor del certificat

El mètode de tramesa de la clau pública a l'EC-URV és PKCS #10

6.1.4 Distribució de la clau pública del Prestador de Serveis de Certificació

La clau de l'EC-URV i les claus de les Entitats de Certificació anteriors en la jerarquia pública de certificació de Catalunya són comunicades als verificadors, assegurant la integritat de la clau i autenticant l'origen.

La clau pública de l'EC-ACC (Entitat de Certificació de l'Agència Catalana de Certificació) que és l'arrel de la jerarquia, es publica en el Dipòsit de l'EC-URV, en forma de certificat auto-signat, al costat d'una declaració referent a que la clau permet autenticar a l'EC-URV.

S'estableixen mesures addicionals per confiar en el certificat auto-signat, com ara la comprovació de l'empremta digital del certificat.

La clau pública de l'EC-URV es publica en el Dipòsit de l'EC-URV, en forma de certificat CIC firmat per CATCert.

Els usuaris accedeixen al Dipòsit per obtenir les claus públiques de l'EC-URV.

Addicionalment, en aplicacions S/MIME, el missatge de dades conté una cadena de certificats, incloent certificats CIC amb les claus públiques de les Entitats de Certificació de la jerarquia, que d'aquesta forma es distribueix als usuaris.

6.1.5 Mesures de claus

Les claus de l'EC-URV és almenys de 2.048 bits.

Les claus dels subscriptors de certificats CPISR i d'entitat (CESR i CEX) de l'EC-URV són almenys de 1.024 bits.

Les claus de la resta de tipus de certificats són almenys de 512 bits.

6.1.6 Generació de paràmetres de clau pública

Sense estipulació addicional.

6.1.7 Comprovació de qualitat de paràmetres de clau pública

Es realitza d'acord amb l'informe especial de l'ETSI SR 001 276, que indica la qualitat dels algoritmes de signatura electrònica.

6.1.8 Generació de claus en aplicacions informàtiques o en bens d'equip

Els parells de claus de l'EC-URV són generats utilitzant maquinari criptogràfic que compleix els requisits establerts per l'especificació tècnica CEN CWA 141617 o equivalent.

Els parells de claus dels subscriptors de certificats CPISR, CPX, CESR i CEX s'han de generar al component d'Autoritat de Registre Local i en targetes intel·ligents. o en dispositius criptogràfics que compleixen els requisits establerts per les especificacions tècniques CEN CWA 14169 i CWA 14170 o equivalent.

L'EC-URV o l'Entitat de Registre comprova l'autenticitat i el nivell de seguretat de les targetes o dispositius criptogràfics adquirits als proveïdors, mitjançant un procediment específic establert a l'efecte, abans d'autoritzar-ne l'ús.

La generació de claus per a la resta de certificats poden realitzar-se mitjançant aplicacions informàtiques.

6.1.9 Propòsits d'ús de claus

L'EC-URV inclou l'extensió KeyUsage a tots els certificats, indicant els usos permesos de les corresponents claus privades.

6.2 Protecció de la clau privada

6.2.1 Estàndards de mòduls criptogràfics

Les claus privades de les Entitats de Certificació (tant de CATCert com de l'EC-URV) es protegeixen utilitzant maquinari criptogràfic que compleix els requisits establerts per l'especificació tècnica FIPS 140-1 Nivell 3 o equivalent.

Els parells de claus dels subscriptors de certificats CPISR, CPX i d'entitat estan protegits per targetes intel·ligents que compleixen els requisits establerts per l'especificació tècnica CEN CWA 14169 o equivalent.

6.2.2 Control per més d'una persona (n de m) sobre la clau privada

Dels 5 possibles dispositius criptogràfics que existeixen l'EC-URV requereix la concurrència d'almenys 2 de forma simultània.

Cada un d'aquests dispositius és responsabilitat d'una persona concreta, única coneixedora de la clau d'accés al mateix. La clau d'accés és coneguda únicament per una persona responsable d'aquest dispositiu. Cap d'elles no en coneix més que una de les claus d'accés.

Els dispositius criptogràfics queden emmagatzemats a les dependències de l'EC-URV, i per al seu accés és necessària una persona addicional.

6.2.3 Dipòsit de la clau privada

Les claus privades de l'EC-URV s'emmagatzemen en espais ignífugs i protegits per controls d'accés físic doble.

Les claus privades dels certificats CPX i CEX sí es poden emmagatzemar a l'EC-URV.

6.2.4 Còpia de seguretat de la clau privada

Existeix còpia de seguretat de la clau privada de l'EC-URV i dels mitjans necessaris per accedir, en lloc independent d'aquella on s'emmagatzema habitualment.

6.2.5 Arxiu de la clau privada

La clau privada de l'EC-URV compta amb una còpia de seguretat realitzada, emmagatzemada, i recuperada en el seu cas per personal subjecte a la política de confiança del personal. Aquest personal està expressament autoritzat per a aquestes finalitats, i es limita a aquell que necessiti fer-ho en les pràctiques de l'EC-URV.

Els controls de seguretat a aplicar en còpies de seguretat de l'EC-URV són d'igual o superior nivell a les que s'apliquin a les claus habitualment en ús.

Quan les claus s'emmagatzemen en un mòdul maquinari de procés dedicat, han de proveir-se els controls oportuns perquè aquestes mai no puguin abandonar el dispositiu.

No s'emmagatzemen còpies de les claus privades dels certificats, excepte en el cas dels certificats CPX, per garantir la recuperació de les dades i sempre que així ho indiqui el subscriptor.

6.2.6 Introducció de la clau privada en el mòdul criptogràfic

Les claus privades de l'EC-URV queden emmagatzemades en fitxers xifrats amb claus fragmentades i en targetes intel·ligents (de les quals no poden ser extretes).

Aquestes targetes són utilitzades per introduir la clau privada en el mòdul criptogràfic.

6.2.7 Emmagatzematge de la clau privada en el mòdul criptogràfic

Les claus privades es generen directament en els mòduls criptogràfics.

6.2.8 Mètode d'activació de la clau privada.

Es requereixen almenys dues persones per activar la clau privada de l'EC-URV.

Per a certificats personals i d'entitat, la clau privada del subscriptor s'activa mitjançant la introducció del PIN a la targeta intel·ligent.

6.2.9 Mètode de desactivació de la clau privada

No aplicable.

6.2.10 Mètode de destrucció de la clau privada

Les claus privades són destruïdes de manera que s'impedeixi el seu robatori, modificació, divulgació no autoritzada o ús no autoritzat.

6.2.11 Classificació dels mòduls criptogràfics

Els mòduls de l'EC-URV obtenen o superen el nivell EAL 4 de Common Criteria (ISO 15408) amb els augments que determinen a l'especificació tècnica CEN CWA 14167 o equivalent.

Els mòduls dels subscriptors de certificats CPISR, CPX, CESR i CEX obtenen o superen el nivell EAL 4 de Common Criteria (ISO 15408) amb els augments que determinen a l'especificació tècnica CEN CWA 14169 o equivalent.

6.3 Altres aspectes de gestió del parell de claus

6.3.1 Arxiu de la clau pública

L'EC-URV arxiva les seves claus públiques, d'acord amb l'establert a la secció 4.12.

6.3.2 Períodes d'utilització de les claus pública i privada

Els períodes d'utilització de les claus són les determinades per la durada del certificat, i una vegada transcorregut no es poden continuar utilitzant.

Com a excepció, la clau privada de desxifrat pot continuar utilitzant-se fins després de l'expiració del certificat.

6.4 Dades d'activació

6.4.1 Generació i instal·lació de les dades d'activació

L'EC-URV, atès que la URV disposa d'una Entitat de Registre Interna, quan el posseïdor es presenta a l'Entitat de Registre Interna amb la targeta criptogràfica (carnet URV), se li creen o canvien les dades d'activació.

6.4.2 Protecció de dades d'activació

6.4.2.1 Per a certificats personals i d'entitat.

Donat que la URV disposa d'Entitat de Registre Interna, per protegir al màxim les dades d'activació, quan el posseïdor de claus es presenta físicament davant l'Entitat de Registre Interna, aquesta crea en la seva presència les dades d'activació de signatura o en tot cas es canvien.

6.4.2.2 Per a certificats de servidor

La distribució de les dades d'activació per als certificats de servidor és idèntica a la dels certificats personals, amb la diferència, que només s'inclou la clau pública ja que la privada la genera el propi subscriptor que ha demanat el certificat.

6.4.3 Altres aspectes de les dades d'activació

Sense estipulació addicional.

6.5 Controls de seguretat informàtica

6.5.1 Requisits tècnics específics de seguretat informàtica

Es garanteix que l'accés als sistemes és limitat a individus degudament autoritzats. En particular:

- L'EC-URV garanteix una administració efectiva del nivell d'accés dels usuaris (operadors, administradors, així com de qualsevol usuari amb accés directe al sistema) per mantenir la seguretat del sistema, incloent la gestió de comptes d'usuari, auditoria i modificacions o denegacions d'accés oportunes.

- L'EC-URV garanteix que l'accés als sistemes d'informació i aplicacions es restringeix d'acord a l'establert en la política de control d'accés, així com que els sistemes proporcionen els controls de seguretat suficients per implementar la segregació de funcions identificada en les pràctiques de l'EC-URV, incloent la separació de funcions d'administració dels sistemes de seguretat i dels operadors. En concret, l'ús de programes d'utilitats del sistema està restringit i estretament controlat.

- El personal de l'EC-URV està identificat i reconegut abans d'utilitzar aplicacions crítiques relacionades amb el cicle de vida del certificat.

- El personal de l'EC-URV és responsable i pot justificar les seves activitats, per exemple mitjançant un arxiu d'esdeveniments.

- Ha d'evitar-se la possibilitat de revelació de dades sensibles mitjançant la reutilització d'objectes d'emmagatzematge (per exemple fitxers esborrats) que quedin accessibles a usuaris no autoritzats.

- Els sistemes de seguretat i monitoratge permeten una ràpida detecció, registre i actuació davant d'intents d'accés irregulars o no autoritzats als seus recursos (per exemple, mitjançant un sistema de detecció d'intrusions, monitoratge i alarma).

- L'accés als dipòsits públics de la informació de l'EC-URV (per exemple, certificats o informació d'estat de revocació) conta amb un control d'accessos per a modificacions o esborrament de dades.

6.5.2 Avaluació del nivell de seguretat informàtica

Les aplicacions de CA i RA són fiables, d'acord amb l'especificació tècnica CEN CWA 14167-1, avaluant-se el grau de compliment mitjançant una auditoria de seguretat informàtica conforme amb l'especificació tècnica CEN CWA 14172-3 i un perfil de protecció adequat, d'acord amb la norma ISO 15408 o equivalent.

6.6 Controls tècnics del cicle de vida

6.6.1 Controls de desenvolupament de sistemes

Es realitza una anàlisi de requisits de seguretat durant les fases de disseny i especificació de requisits de qualsevol component de l'EC-URV i de les Entitats de Registre, utilitzat en les aplicacions d'Autoritat (tècnica) de certificació i d'Autoritat (tècnica) de Registre, per garantir que els sistemes són segurs.

S'utilitzen procediments de control de canvis per a les noves versions, actualitzacions i pegats d'emergència, dels esmentats components.

6.6.2 Controls de gestió de seguretat

L'EC-URV garanteix que les seves funcions de gestió de les operacions dels mòduls criptogràfics són suficientment segures, i en particular, ha d'assegurar que existeixen instruccions per:

a. Operar els mòduls de forma correcta i segura.
b. Instal·lar els mòduls minimitzant el risc de fallada dels sistemes.
c. Protegir els mòduls contra virus i programari maliciós, per garantir la integritat i validesa de la informació que processen.

L'EC-URV manté un inventari de tots els actius informàtics i realitza una classificació dels mateixos d'acord amb les seves necessitats de protecció, coherent amb l'anàlisi de riscs efectuada.

La configuració dels sistemes s'audita de forma periòdica, d'acord amb l'establert a la secció 8.1

Es realitza un seguiment de les necessitats de capacitat, i es planificaran procediments per garantir suficient disponibilitat electrònica i d'emmagatzematge per als actius informatius.

6.6.3 Avaluació del nivell de seguretat del cicle de vida

Sense estipulació addicional.

6.7 Controls de seguretat de xarxa

Es garanteix que l'accés a les diferents xarxes de l'EC-URV és limitat a individus degudament autoritzats. En particular:

- S'implementen controls (com per exemple tallafocs) per protegir la xarxa interna de dominis externs accessibles per terceres parts. Els tallafocs es configuren de manera que s'impedeixin accessos i protocols que no siguin necessaris per a l'operació de l'EC-URV.

- Les dades sensibles es protegeixen quan s'intercanvien a través de xarxes no segures (incloent les dades de registre del subscriptor).

- Es garanteix que els components locals de xarxa (com encaminadors) es troben ubicats en entorns segurs, així com l'auditoria periòdica de les seves configuracions.

6.8 Segell de temps

Sense estipulació addicional.

7. Perfils de certificats i llistes de certificats revocats

7.1 Perfil de certificat

Aquesta secció es troba en la web (***www.catcert.net/registre***)

7.2 Perfil de la llista de revocació de certificats

Aquesta secció es troba en la web (***www.catcert.net/registre***)

8. Auditoria de conformitat

L'EC-URV realitza periòdicament una auditoria de conformitat per provar que compleix els requisits de seguretat i d'operació necessaris per formar part de la jerarquia pública de certificació de Catalunya.

L'EC-URV pot delegar l'execució de les auditories a CATCert o a una tercera entitat contractada per CATCert. En aquest cas l'EC-URV coopera completament amb el personal que porta a terme la investigació.

8.1 Freqüència de l'auditoria de conformitat

L'EC-URV porta a terme una auditoria de conformitat anualment, a més de les auditories internes que realitza sota el seu propi criteri o en qualsevol moment, a causa d'una sospita d'incompliment d'alguna mesura de seguretat o per un compromís de claus.

8.2 Identificació i qualificació de l'auditor

La Entitat de Registre Interna, pot encarregar-se de realitzar l'auditoria de conformitat.

No obstant això l'EC-URV pot acudir a un auditor independent extern, el qual ha de demostrar experiència en seguretat informàtica, en seguretat de Sistemes d'Informació i en auditories de conformitat d'Autoritats de Certificació i els elements relacionats.

8.3 Relació de l'auditor amb l'entitat auditada

Les auditories de conformitat executades per tercers estan realitzades per una entitat independent de l'EC-URV auditada, que no té cap conflicte d'interessos que afecti negativament la seva capacitat de realitzar serveis d'auditoria.

8.4 Relació d'elements objecte d'auditoria

Els elements objecte d'auditoria són els següents:

- Processos d'Autoritats de Certificació i elements relacionats
- Sistemes d'informació
- Protecció del centre de procés
- Documents

8.5 Accions a emprendre com a resultat d'una falta de conformitat

Una vegada rebut l'informe de l'auditoria de compliment ja realitzada, l'EC-URV discuteix, amb l'entitat que ha executat l'auditoria i amb CATCert, les deficiències trobades i desenvolupa i executa un pla correctiu que soluciona les esmentades deficiències.

Si l'EC-URV un cop auditada és incapaç de desenvolupar i/o executar l'esmentat pla o si les deficiències trobades suposen una amenaça immediata per a la seguretat o integritat del sistema es realitza una de les següents accions:

- Revocar la clau de l'EC-URV, de la forma com es descriu a la secció 4.9
- Acabar el servei de l'EC-URV, de la forma com es descriu a la secció 5.8

8.6 Tractament dels informes d'auditoria

L'EC-URV lliura els informes de resultats d'auditoria a CATCert en qualitat d'Entitat de Certificació Arrel de la jerarquia pública de certificació de Catalunya, en un termini màxim de 15 dies després de l'execució de l'auditoria.

9. Requisits comercials i legals

9.1 Tarifes

9.1.1 Tarifa d'emissió o renovació de certificats

El Consell de Govern de la Universitat Rovira i Virgili de comú acord amb CATCert estableix les tarifes que aplica l'EC-URV, en la prestació dels seus serveis.

9.1.2 Tarifa d'accés a certificats

No es pot establir una tarifa per l'accés als certificats.

9.1.3 Tarifa d'accés a informació d'estat de certificat

No es pot establir una tarifa per l'accés a la informació d'accés als certificats.

9.1.4 Tarifes d'altres serveis

Sense estipulació addicional

9.1.5 Política de reintegrament

Sense estipulació addicional.

9.2 Capacitat financera

9.2.1 Assegurança de responsabilitat civil

L'EC-URV disposa d'una garantia de cobertura de la seva responsabilitat civil suficient, en els termes previstos a l'article 20.2 de la Llei 59/2003, de 19 de desembre.

9.2.2 Altres actius

Sense estipulació addicional.

9.2.3 Cobertura d'assegurament per a subscriptors i tercers que confien en certificats

La cobertura l'aporta l'assegurança prevista a l'apartat 9.2.1, pels danys previstos per la Llei 59/2003, de 19 de desembre, excloses les exoneracions legals de responsabilitat que preveu el seu article 23.

9.3 Confidencialitat

9.3.1 Informacions confidencials

Les següents informacions són mantingudes confidencials per l'EC-URV:

a. Informació de negoci subministrada pels seus proveïdors i altres persones amb qui CATCert o l'EC-URV tenen una obligació de guardar secret, establerta legalment o convencionalment.

b. Registres de transaccions, incloent els registres complets i els registres d'auditoria de les transaccions.

c. Registres d'auditoria interna i externa, creats i/o mantinguts per l'EC-URV i els seus auditors.

d. Plans de continuïtat de negoci i d'emergència.

e. Política i plans de seguretat

f. Documentació d'operacions i restants plans d'operació, com ara arxiu, monitoratge i altres d'anàlegs.

g. Tota altra informació identificada com "Confidencial"

9.3.2 Informacions no confidencials

Les següents informacions no tenen caràcter confidencial:

a. La política de certificació de l'EC-URV

b. La Declaració de Pràctiques de Certificació de l'EC-URV

c. Tota altra informació identificada com "Pública"

9.3.3 Responsabilitat per la protecció d'informació confidencial

L'EC-URV és responsable de l'establiment de les mesures apropiades de protecció de la informació confidencial.

Aquestes mesures inclouen les clàusules apropiades d'informació confidencials als instruments jurídics amb totes les persones.

9.4 Protecció de dades personals

9.4.1 Pla de Protecció de Dades Personals

L'EC-URV desenvolupa una política d'intimitat, d'acord amb la Llei Orgànica 15/99, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

L'EC-URV no divulga ni cedeix dades personals, excepte en els casos previstos, així com en la secció 5.8, en cas d'acabament de l'Entitat de Certificació.

L'EC-URV disposa dels procediments en aquest document, que aplica en la prestació dels seus serveis, en el qual, en compliment dels requisits establerts per les polítiques de certificats que gestiona, i d'acord amb l'article 19 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, es detallen els requisits i obligacions en relació amb l'obtenció i gestió de les dades personals que obtingui, complint a aquest efecte, les disposicions de la Llei Orgànica 15/1999 de 13 de desembre, de Protecció de Dades de Caràcter Personal, i del Reial Decret 994/1999, d'11 de juny, que aprova el Reglament de Mesures de Seguretat dels fitxers automatitzats que continguin dades de caràcter personal.

En concret, les següents seccions del Reglament de Mesures de Seguretat es compleixen amb els controls de les següents seccions d'aquest document:

a. Àmbit d'aplicació del document de seguretat amb especificació detallada dels recursos protegits - secció 9.4
b. Mesures, normes, procediments, regles i estàndards que garanteixin el nivell de seguretat exigit pel Reglament - secció 9.4, i, en general, tots els controls tècnics de les seccions 5 i 6.
c. Funcions i obligacions del personal - secció 5.3
d. Estructura dels fitxers amb dades de caràcter personal i descripció dels sistemes d'informació que els tractin - secció 9.4.2 i secció 1.3.1 respectivament.
e. Procediment de notificació, gestió i resposta davant de les incidències - secció 9.4.4
f. Procediments de còpia de seguretat i recuperació de dades - secció 5.5

9.4.2 Informació considerada privada

De conformitat amb l'establert a l'article 3 de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, es consideren dades de caràcter personal qualsevol informació relativa a persones físiques identificades o identificables.

La informació personal que no hagi de ser inclosa als certificats i al mecanisme indicat de comprovació de l'estat dels certificats, és considerada informació personal de caràcter privat.

Les següents dades són considerades en tot cas com a informació privada:

- Sol·licituds de certificats, aprovades o denegades, així com tota altra informació personal obtinguda per a l'expedició i manteniment de certificats.
- Claus privades generades i/o emmagatzemades per l'EC-URV.
- Tota altra informació identificada com "Informació privada"

En qualsevol cas, les dades captades pel prestador de serveis de certificació tenen la consideració legal de dades de nivell bàsic.

La informació confidencial d'acord amb la LOPD és protegida de la seva pèrdua, destrucció, dany, falsificació i processament il·lícit o no autoritzat, d'acord amb les prescripcions establertes al Reial Decret 994/99, d'11 de juny, pel qual s'aprova el Reglament de Mesures de seguretat dels fitxers automatitzats que continguin dades de caràcter personal.

En cap cas l'EC-URV no inclou als certificats electrònics que expedeix, les dades a què es fa referència a l'article 7 de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

L'estructura dels arxius de dades personals de l'EC-URV és la següent:

Estructura de l'arxiu	
Dades de caràcter identificatiu :	
Del subscriptor	- NIF - Nom

Del Certificador	- NIF - Nom i cognoms
Del Posseïdor de claus	- ID (NIF o similar) - Nom i cognoms - Direcció postal - Direcció electrònica - Fotografia - Categoria - Càrrec

9.4.3 Informació no considerada privada

Aquesta informació es tracta d'informació personal que s'inclou als certificats i al referit mecanisme de comprovació de l'estat dels certificats, d'acord amb la secció 3.1 d'aquest document.

L'esmentada informació, proporcionada a la sol·licitud de certificats en els termes que es preveuen a l'article 17.2 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, és inclosa als seus certificats i al mecanisme de comprovació de l'estat dels certificats.

La informació no té caràcter privat, per imperatiu legal ("dades públiques"), però sol es publica en el dipòsit si ho consenteix el subscriptor.

En tot cas, és considerada no confidencial la següent informació:

a. Els certificats emesos o en tràmit d'emissió
b. La subjecció del subscriptor a un certificat emès per l'EC-URV.
c. El nom i els cognoms del subscriptor del certificat, així com qualssevol altres circumstàncies o dades personals del titular, en el supòsit, que siguin significatives en funció de la finalitat del certificat, d'acord amb aquest document.
d. La direcció electrònica del subscriptor del certificat.
e. Els usos i límits econòmics ressenyats al certificat.
f. El període de validesa del certificat, així com la data d'emissió del certificat i la data de caducitat.
g. El número de sèrie del certificat.
h. Els diferents estats o situacions del certificat i la data de l'inici de cada un d'ells, en concret: pendent de generació i/o lliurament, vàlid, revocat, suspès o caducat i el motiu que va provocar el canvi d'estat.
i. Les llistes de revocació de certificats (LRCs), així com la resta d'informacions d'estat de revocació.
j. La informació continguda en la part pública del Dipòsit de l'EC-URV.

9.4.4 Responsabilitat corresponent a la protecció de les dades personals

L'EC-URV, com a mínim, garanteix el compliment de les seves obligacions legals com a prestador de serveis de certificació, de conformitat amb la Llei 59/2003, de 19 de desembre, i en virtut d'això, i d'acord amb l'article 22 de l'esmentada Llei, respon pels danys i perjudicis que causi a l'exercici de l'activitat que li és pròpia, en el cas d'incomplir, en allò que aquí interessa, les obligacions contingudes a l'article 17 de la Llei 59/2003, relatives a la protecció de dades personals.

L'EC-URV inclou en aquest document el seu procediment de notificació, gestió i resposta davant de les incidències relacionades amb les dades personals.

Aquest procediment de notificació s'inicia quan l'administrador dels sistemes de l'EC-URV, a les seves instal·lacions, comunica immediatament per telèfon amb el Responsable de l'Àrea Tècnica de l'EC-URV, descrivint el tipus d'incidència i els efectes que s'observen.

Si durant la gestió de la incidència fa falta fer modificacions del programari o en la configuració dels sistemes, o cal restaurar còpies de seguretat o altres intervencions semblants, l'administrador s'espera fins i tot rebre la petició corresponent per correu electrònic firmat digitalment, i que l'envia el Responsable de l'Àrea Tècnica o el responsable tècnic del projecte afectat (en aquest cas amb còpia del missatge al Responsable de l'Àrea Tècnica).

Una vegada fetes les actuacions necessàries i restablert el normal funcionament dels sistemes, l'administrador dels sistemes envia per correu electrònic dirigit al Responsable de l'Àrea Tècnica un informe descriptiu, que en el cas de les incidències produïdes sobre fitxers que contenen dades de caràcter personal, no és més que el formulari tipus degudament emplenat.

El Responsable de l'Àrea Tècnica manté còpia dels formularis corresponents a les incidències registrades durant els 12 últims mesos sobre els fitxers que contenen dades de caràcter personal. Aquests es guarden en un directori dedicat dins del servidor que comparteixen els usuaris de l'EC-URV, protegit convenientment perquè només pugui accedir el personal de l'Àrea Tècnica; així queda garantit que es fan còpies de seguretat del seu contingut.

Al formulari de Registre d'Incidències es fan constar les següents dades:

- Quin recurs té la incidència
- El seu codi i descripció
- El dia i l'hora
- El tipus d'incidència
- Els efectes
- El comunicant i el destinatari
- La resposta
- Els procediments previstos a realitzar
- La persona que els realitzarà.
- Procediment per la recuperació

- Persona (i autorització) per la recuperació
- Les dades restaurades.

L'EC-URV implanta mesures d'identificació i autenticació, així com el necessari control d'accés del personal a les dades personals, controls que detallen les seccions 4 i 5 d'aquest document.

Els procediments de gestió dels suports de dades personals i de les còpies de seguretat definits a les seccions 5.5 d'aquest document compleixen els requisits dels articles 13 i 14 del Reial Decret 994/99.

9.4.5 Prestació del consentiment en l'ús de les dades personals

Per a la prestació del servei, l'EC-URV necessita recollir i emmagatzemar certes informacions, que inclouen informacions personals.

En l'expedició de certificats de l'EC-URV de classe 1 (amb càrrec) i de classe 2 (d'estudiant), aquestes informacions són comunicades pels subscriptors, sense necessitat de consentiment exprés dels posseïdors de claus, d'acord amb l'establert per la normativa reguladora de la relació del personal al servei del subscriptor del certificat o una altra normativa que resulti aplicable, com preveu l'articulo 11 de la LOPD.

L'EC-URV informa els posseïdors de claus de l'obtenció de les seves dades personals.

9.4.6 Divulgació de la informació originada per procediments administratives i/o judicials

L'EC-URV divulga la informació confidencial en els casos legalment previstos per a aquest tema.

En concret, l'EC-URV està obligada a revelar la identitat dels signants quan el sol·licitin els òrgans judicials en l'exercici de les funcions que tinguin atribuïdes i en la resta de supòsits previstos a l'article 11.2 de la LOPD on així es requereixi.

L'EC-URV indica aquestes circumstàncies en la política d'intimitat prevista a la secció 9.4.1.

9.4.7 Altres supòsits de divulgació de la informació

L'EC-URV inclou, en la política d'intimitat prevista a la secció 9.4.1, prescripcions per permetre la divulgació de la informació del posseïdor de claus, directament als mateixos o a tercers.

9.5 Drets de propietat intel·lectual

9.5.1 Propietat dels certificats i informació de revocació

L'EC-URV és l'única entitat que gaudeix dels drets de propietat intel·lectual sobre els certificats que emet.

L'EC-URV concedeix llicència no exclusiva per reproduir, distribuir, verificar i utilitzar els certificats, sense cap cost, en relació amb firmes digitals i/o sistemes de xifrat dins de l'àmbit d'aplicació d'aquest document, d'acord amb el corresponent instrument vinculant entre l'EC-URV i la part que reprodueixi i/o distribueixi el certificat.

Les anteriors normes figuren als instruments jurídics que existeixen entre l'EC-URV i els subscriptors i els verificadors.

Addicionalment, els certificats emesos per l'EC-URV contenen un avís legal relatiu a la propietat d'aquests. Aquesta normativa resulta d'aplicació en l'ús d'informació de revocació de certificats.

9.5.2 Propietat de la Política de Certificat i Declaració de Pràctiques de Certificació

CATCert és l'única entitat que gaudeix dels drets de propietat intel·lectual sobre la política de certificació de la jerarquia pública de certificació de Catalunya.

L'EC-URV és propietària d'aquesta Declaració de Pràctiques de Certificació.

9.5.3 Propietat de la informació relativa a noms

El subscriptor (o el posseïdor de claus, si procedeix), conserva qualsevol dret, d'existir aquest, relatiu a la marca, producte o nom comercial contingut al certificat.

El subscriptor (o el posseïdor de claus, si procedeix), és el propietari del nom distingit del certificat, format per les informacions especificades a la secció 3.1.

9.5.4 Propietat de claus

Els parells de claus són propietat del subscriptor dels certificats.

Quan una clau es trobi fraccionada en parts, totes les parts de la clau són propietat del propietari de la clau.

9.6 Obligacions i responsabilitat civil

9.6.1 EC-URV

9.6.1.1 Obligacions i altres compromisos

9.6.1.1.1 Obligacions de l'EC-URV

L'EC-URV s'obliga a complir el següent:

- Garanteix sota la seva plena responsabilitat, que compleix amb tots els requisits establerts en aquest document.
- És l'única entitat responsable del compliment dels procediments descrits en aquest document, inclòs quan una part o la totalitat de les operacions siguin sub-contractades externament.
- Presta els seus serveis de certificació d'acord amb aquest document on es detallen almenys els continguts previstos en l'articulo 19 de la Llei 59/2003
- Informa, dels aspectes previstos en l'articulo 18. b) de la Llei 59/2003, i dels següents aspectes:

- Indicació de la política aplicable, amb indicació que els certificats no s'expedeixen al públic i de la necessitat d'utilització de dispositiu segur de creació de firma.
- Forma en que es garanteix la responsabilitat patrimonial per part de l'EC-URV
- L'EC-URV es declara d'acord amb la política de certificació, la certificació del prestador de serveis de certificació i la certificació dels productes de signatura electrònica utilitzats

Aquest requisit es compleix mitjançant un "Text divulgatiu de la política de certificat" aplicable, que es transmet electrònicament, utilitzant un mitjà de comunicació durador en el temps, i en llenguatge comprensible.

- Obliga, als posseïdors de claus i als verificadors mitjançant instruments jurídics apropiats a cada situació, els quals es transmeten electrònicament, en llenguatge escrit i comprensible, i tenint els següents continguts mínims:
  - Prescripcions per donar compliment a l'establert en aquest document.
  - Indicació de la política aplicable, amb indicació de si els certificats s'expedeixen al públic i de la necessitat d'ús del dispositiu segur de creació de firma.
  - Manifestació que la informació continguda al certificat és correcta, excepte notificació en contra pel subscriptor.
  - Consentiment per a la publicació del certificat en el dipòsit i accés per tercers al mateix.
  - Consentiment per a l'emmagatzematge de la informació utilitzada per al registre del subscriptor i del posseïdor de claus, per a la provisió del dispositiu segur de creació de signatura i per a la cessió de la informació esmentada en tercers, en cas de final d'operacions de l'EC-URV sense revocació de certificats vàlids.
  - Límits d'ús del certificat, incloent les establertes a la secció 4.5 d'aquest document.
  - Informació sobre com validar un certificat, incloent el requisit de comprovar l'estat del certificat, i les condicions en les quals es pot confiar raonablement en el certificat, que resulta aplicable quan el subscriptor actua com a verificador.
  - Limitacions de responsabilitat aplicables, incloent els usos pels quals l'EC-URV accepta o exclou la seva responsabilitat.
  - Procediments aplicables de resolució de disputes.
  - Llei aplicable i jurisdicció competent.
  - Identifica el posseïdor de claus, d'acord amb els articles 12 i 13 de la Llei 59/2003 i la present Declaració de Pràctiques de Certificació (DPC) i, Comprova que el posseïdor de la clau es troba degudament autoritzat .
- Compleix la resta d'obligacions contingudes a l'article 12 de la Llei 59/2003

9.6.1.1.1.1 Informació per als certificats personals

L'EC-URV assumeix aquelles altres obligacions incorporades directament al certificat o incorporades per referència.

Nota: La incorporació per referència s'aconsegueix incloent en el certificant un identificador d'objecte o una altra forma d'enllaç en un document, que es considera inclòs de forma integra en la present política de certificat.

L'instrument jurídic que vincula l'EC-URV i el subscriptor està en llenguatge escrit i comprensible, i té els següents continguts mínims:

- Indicació de la política aplicable, amb indicació si els certificats s'expedeixen al públic o a una comunitat tancada d'usuaris i de la necessitat d'ús de dispositiu segur de creació de firma.
- Certificació de serveis de l'EC-URV.
- Manera en què es garanteix la responsabilitat patrimonial de l'EC-URV.

9.6.1.1.1.2 Informació addicional per al CDS i el CDSCD

L'EC-URV comprova el nom de domini, i altres dades tècniques, com la IP, que figuren al certificat.

Les obligacions anteriors s'exerciten dins del marc de les polítiques, pràctiques i normatives generals de la jerarquia pública de certificació de Catalunya.

9.6.1.2 Garanties ofertes a subscriptors i verificadors

L'EC-URV, com a mínim, garanteix al verificador:

a. El compliment de les seves obligacions legals com a prestador de serveis de certificació, d'acord amb la Llei 59/2003, de 19 de desembre.
b. Que la informació continguda o incorporada per referència al certificat és correcta, excepte quan s'indiqui el contrari.
c. En cas de certificats publicats en el Dipòsit, que el certificat ha estat emès al subscriptor identificat en aquest i que el certificat ha estat acceptat, d'acord amb la secció 4.4 del present document.
d. Que en l'aprovació de la sol·licitud de certificat i en l'emissió del certificat s'han complert tots els requisits materials establerts en aquest document.
e. La rapidesa i seguretat en la prestació dels serveis, en especial dels serveis de revocació i Dipòsit
f. Que el certificat conté les informacions que ha de contenir un certificat reconegut, d'acord amb l'article 11.2 de la Llei 59/2003, de 19 de desembre.
g. Que, en el cas que generi les claus privades del subscriptor o, en el seu cas, del posseïdor de claus, es manté la seva confidencialitat durant el procés.
h. La responsabilitat de l'EC-URV, amb els límits que s'estableixin.

9.6.2 Entitat de Registre Interna

9.6.2.1 Obligacions i altres compromisos

L'Entitat de Registre Interna s'obliga a complir el següent:

a. Actua exclusivament en relació amb persones vinculades a l'Entitat de Registre.

b. Nomenar com a operador de l'autoritat de registre, a quatre o a més dels seus treballadors, i comunicar a CATCert les dades corresponents a aquestes persones per a l'emissió dels certificats CIPISR corresponent. Quan un operador deixa de tenir capacitat per actuar com el que és, sota el control i l'autoritat de l'Entitat de Registre, aquesta Entitat sol·licita de forma immediata a la revocació del certificat de CIPISR corresponent.

c. Valida i aprova les sol·licituds de certificats, d'acord amb els procediments i instruments tècnics establerts per l'EC-URV, d'acord amb aquest document i la documentació d'operacions de l'EC-URV.

d. Si l'Entitat de Registre Interna no disposa d'informació actualitzada del posseïdor de claus, comprova la identitat personalment o d'acord amb l'establert a l'article 13.4 de la Llei 59/2003, registra un justificant acreditatiu del nom complet, lloc i data de naixement, DNI i/o qualsevol altra informació que pugui ser utilitzada per diferenciar una persona respecte d'una altra en l'àmbit de l'Entitat de Registre Interna.

e. Verifica, quan sigui necessari, qualsevol atribut específic del posseïdor de claus, i registrar un justificant acreditatiu de la informació.

f. Tramita les sol·licituds de suspensió, reactivació, revocació i renovació de certificats, d'acord amb els procediments i els instruments tècnics establerts per l'EC-URV, d'acord amb aquest document, i la documentació d'operacions de l'EC-URV.

g. Emmagatzema els registres, ja sigui en paper, ja siguin de forma electrònica, amb les adequades mesures de seguretat, autenticitat, integritat i conservació, relatius a la informació continguda al certificat, durant un període de 15 anys. Aquests registres estan a disposició de l'EC-URV.

h. Genera la justificació documental necessària per al registre d'usuaris i per la posterior emissió de certificats .

i. La justificació documental es realitza per una unitat orgànica de l'Entitat de Registre facultada legalment per donar fe de les dades a certificar, que s'indiquen a CATCert.

9.6.3 CATCert

9.6.3.1.1 Garanties ofertes a subscriptors i verificadors

CATCert garanteix que la clau privada de l'EC-URV utilitzada per emetre certificats no està compromesa, a excepció de que CATCert no comuniqui el contrari mitjançant el Dipòsit de CATCert.

CATCert únicament garanteix que:

a) Els certificats contenen tota la informació exigida per la Llei 59/2003, de 19 de desembre.

b) CATCert no ha originat ni ha introduït declaracions falses o errònies en 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, en el moment de l'emissió del certificat.

c) Tots els certificats compleixen els requisits formals i de contingut.

d) CATCert queda vinculada pels procediments operatius i de seguretat descrits en aquest document i al conveni entre CATCert, el CESCA i la URV.

9.6.3.1.2 Exclusió de la garantia

CATCert no garanteix cap programari utilitzat pel subscriptor o per qualsevol altra persona, per generar, verificar o no utilitzar de forma diferent, cap signatura digital o certificat digital emès per CATCert, a excepció dels casos en els quals hi hagi una declaració escrita de CATCert en sentit contrari.

9.6.4 Subscriptors

9.6.4.1 Obligacions i altres compromisos

9.6.4.1.1 Informacions per a tots els tipus de certificats

El subscriptor dels certificats, s'obliga a:

a. Manifestar el seu consentiment previ a l'emissió i lliurament d'un certificat.
b. Complir les obligacions que s'estableixen per al subscriptor en aquest document i a l'article 23.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.
c. Utilitzar el certificat d'acord amb l'establert a la secció 1.4.
d. Obligar als posseïdors de claus a:
    a) Facilitar a l'EC-URV informació completa i adequada, en especial pel que respecta al procediment de registre.
    b) Notificar a l'EC-URV, sense retards injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu segur de creació de firma.
    c) Notificar a l'EC-URV i qualsevol persona que el subscriptor cregui que pugui confiar en el certificat, sense retards injustificables:
        a La pèrdua, el robatori o el compromís potencial de la seva clau privada.
        b La pèrdua de control sobre la seva clau privada, a causa del compromís de les dades d'activació (per exemple, el codi PIN del dispositiu segur de creació de firma) o per qualsevol altra causa.

c Les inexactituds o canvis en el contingut del certificat que conegui o pogués conèixer el subscriptor.

d) Deixar d'utilitzar la clau privada transcorregut el període indicat a la secció corresponent.

e) No monitoritzar, manipular o realitzar actes d'enginyeria inversa sobre la implantació tècnica de la jerarquia pública de certificació de Catalunya, sense permís previ per escrit.

f) No comprometre intencionadament la seguretat de la jerarquia pública de certificació de Catalunya.

9.6.4.1.2 Informacions específiques per al CPISR i el CESR

El subscriptor s'obliga a:

a. Utilitzar el parell de claus exclusivament per a firmes electròniques i conforme a qualsevol altres limitacions que li siguin notificades.

b. Reconèixer que aquestes firmes electròniques són firmes electròniques equivalents a firmes manuscrites, d'acord amb l'article 3.4 de la Llei 59/2003, de 19 de desembre.

c. Ser especialment diligent en la custòdia de la seva clau privada i del seu dispositiu segur de creació de firma, a fi d'evitar usos no autoritzats

d. Notificar a l'EC-URV, sense retards injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu segur de creació de firma.

e. El subscriptor genera les seves pròpies claus, per tant, s'obliga a:

   a. Generar les seves claus de subscriptor utilitzant un algoritme reconegut com a acceptable per a la signatura electrònica reconeguda.

   b. Crear les claus dins del dispositiu segur de creació de firma.

   c. Utilitzar longituds i algoritmes de clau reconeguts com a acceptables per a la signatura electrònica reconeguda.

9.6.4.2 Garanties ofertes pel subscriptor

El subscriptor s'obliga a garantir que:

a. Totes les manifestacions realitzades a la sol·licitud són correctes.

b. Totes les informacions subministrades que es trobin contingudes al certificat són correctes.

c. El certificat s'utilitza exclusivament per a usos legals i autoritzats, d'acord amb aquest document.

d. Cada signatura digital creada amb la clau privada corresponent a la clau pública llistada al certificat és la signatura digital del subscriptor i que el certificat ha estat acceptat i es troba operatiu (no ha expirat ni ha estat revocat) en el moment de creació de la firma.

e. És una entitat final i no una Entitat de Certificació, i no utilitza la clau privada corresponent a la clau pública llistada al certificat per signar cap certificat (o qualsevol altre format de clau pública certificada), ni LRC.

f. Cap persona no autoritzada no ha tingut mai accés a la clau privada del subscriptor.

9.6.4.3 Protecció de la clau privada

La URV s'obliga a garantir que és l'únic responsable dels danys causats pel seu incompliment del deure de protegir la clau privada.

9.6.5 Verificadors

9.6.5.1 Obligacions i altres compromisos

L'EC-URV obliga l'usuari de certificats a:

a. Assessorar-se sobre el fet que el certificat és apropiat per a l'ús que es pretén.

b. Verificar la validesa, suspensió o revocació dels certificats emesos, per a la qual cosa utilitza informació sobre l'estat dels certificats.

c. Verificar tots els certificats de la jerarquia de certificats, abans de confiar en la signatura digital o en algun dels certificats de la jerarquia.

d. Tenir present qualsevol limitació en l'ús del certificat, amb independència que es trobi al mateix certificat o al contracte de verificador.

e. Tenir present qualsevol precaució establerta en un contracte o en un altre instrument, amb independència de la seva naturalesa jurídica.

f. No monitoritzar, manipular o realitzar actes d'enginyeria inversa sobre la implantació tècnica de la jerarquia pública de certificació de Catalunya, sense permís previ per escrit.

g. No comprometre intencionadament la seguretat de la jerarquia pública de certificació de Catalunya.

h. Reconèixer que les firmes electròniques produïdes pels certificats reconeguts de signatura reconeguda són firmes electròniques equivalents a firmes escrites, d'acord amb l'art. 3.4 de la Llei 59/2003, de 19 de desembre.

9.6.5.2 Garanties ofertes pel verificador

L'EC-URV obliga al verificador, mitjançant el corresponent instrument jurídic, a manifestar que:

a. Disposa de suficient informació per prendre una decisió informada per confiar o no en el certificat.

b. És l'únic responsable de confiar o no en la informació continguda al certificat.

c. Serà l'únic responsable si incompleix les seves obligacions com a verificador.

9.6.6 Altres participants

9.6.6.1 Obligacions i garanties del Registre de certificació

L'EC-URV pot delegar algunes funcions en el Registre de certificació, que en aquest cas està obligat al seu compliment, en les mateixes condicions que l'Entitat de Certificació. Les funcions, obligacions i deures del Registre s'estableixen detalladament en aquest document, així com en la documentació jurídica auxiliar, especialment la lliurada a subscriptors, posseïdors de claus i verificadors.

9.6.6.2 Garanties ofertes pel Registre de certificació

L'EC-URV estableix en aquest document la responsabilitat civil del Registre de certificació, quan sigui operat per una tercera entitat.

9.7 Renúncies de garanties

9.7.1 Rebuig de garanties de la EC-URV

L'EC-URV rebutja totes les garanties del servei, que no es trobin vinculades a obligacions establertes per la Llei 59/2003, de 19 de desembre, incloent especialment la garantia d'adaptació per a un propòsit particular o garantia d'ús mercantil del certificat.

9.8 Limitacions de responsabilitat

9.8.1 Limitacions de responsabilitat de la EC-URV

L'EC-URV limita la seva responsabilitat restringint el servei a l'emissió i gestió de certificats i, en el seu cas, de parells de claus de subscriptors i dipòsits criptogràfics (de signatura i verificació de firma, així com de xifrat o desxifrat).

L'EC-URV no limita la seva responsabilitat mitjançant la inclusió de límits d'ús del certificat, i límits de valor de les transaccions per a les quals pot utilitzar-se el certificat.

9.8.2 Cas fortuït i força major

L'EC-URV inclou clàusules per limitar la seva responsabilitat en cas fortuït i en cas de força major, als instruments jurídics amb què vinculi subscriptors i verificadors.

9.9 Indemnitzacions

9.9.1 Clàusula d'indemnitat de subscriptor

No s'estableix clàusula d'indemnitat del subscriptor.

9.9.2 Clàusula d'indemnitat de verificador

No s'estableix clàusula d'indemnitat del verificador.

9.10 Termini i acabament

9.10.1 Termini

L'EC-URV estableix, als seus instruments jurídics amb els subscriptors i els verificadors, una clàusula que determina el període de vigència de la relació jurídica en virtut de la qual subministra certificats als subscriptors.

9.10.2 Finalització

L'EC-URV estableix, als seus instruments jurídics amb els subscriptors i els verificadors, una clàusula que determina les conseqüències de l'acabament de la relació jurídica en virtut de la que subministra certificats als subscriptors.

9.10.3 Supervivència

L'EC-URV estableix, als seus instruments jurídics amb els subscriptors i els verificadors, clàusules de supervivència, en virtut de la qual certes regles continuen vigents després de l'acabament de la relació jurídica reguladora del servei entre les parts.

A aquest efecte, l'EC-URV vetlla perquè, almenys els requisits continguts a les seccions Obligacions i Responsabilitat civil (9.6), Auditoria de conformitat (8) i Confidencialitat (9.3), continuïn vigents després de l'acabament de la política de certificació i dels instruments jurídics que vinculen l'EC-URV amb subscriptors i verificadors.

9.11 Notificacions

L'EC-URV estableix, als seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules de notificació.

En virtut de la clàusula de notificació s'estableix el procediment pel que les parts es notifiquin fets mútuament.

9.12 Modificacions

9.12.1 Procediment per a les modificacions

L'EC-URV pot modificar, de forma unilateral, aquest document, sempre que procedeixi segons el següent procediment:

- La modificació ha d'estar justificada des del punt de vista tècnic, legal o comercial.
- La modificació proposada per l'EC-URV no pot anar en contra de la política de certificació establerta per CATCert.
- S'estableix un control de modificacions, per garantir, en tot cas, que les especificacions resultants compleixen els requisits que s'intenten complir i que van donar peu al canvi.

- S'estableixen les implicacions que el canvi d'especificacions té sobre l'usuari, i es preveu la necessitat de notificar-li les esmentades modificacions.
- La nova política ha de ser aprovada per CATCert.

9.12.2 Període i mecanismes per a notificacions

Les modificacions d'aquest document es notifiquen a CATCert, per a la seva posterior aprovació.

9.12.3 Circumstàncies en les que un OID ha de ser canviat

Sense estipulació addicional.

9.13 Resolució de conflictes

9.13.1 Resolució extrajudicial de conflictes

L'EC-URV estableix, als seus instruments jurídics amb els verificadors, els procediments de mediació i resolució de conflictes aplicables .

Amb aquesta finalitat, es té en compte la consideració com a Administració Pública de l'EC-URV, quan sigui aplicable aquesta circumstància.

Les situacions de discrepància que es derivin de l'ús dels certificats emesos per l'EC-URV, es resolen aplicant els mateixos criteris de competència que en els casos dels documents firmats per escrit.

9.13.2 Jurisdicció competent

L'EC-URV estableix, als seus instruments jurídics vinculants amb els verificadors, una clàusula de jurisdicció competent, indicant que la competència judicial internacional correspon als jutges espanyols.

La competència territorial i funcional es determina en virtut de les regles de dret internacional privat i regles de dret processal que resultin d'aplicació.

Quan l'EC-URV tingui la consideració d'Administració Pública es té en compte la legislació administrativa que resulti aplicable.

9.14 Llei aplicable

L'EC-URV estableix, als seus instruments jurídics amb els verificadors, que la llei aplicable a la prestació dels serveis, incloent la política i pràctiques de certificació és la següent:

- En general, la llei espanyola, sempre i quan l'EC-URV continuï establerta en l'Estat Espanyol, i/o els seus serveis de certificació es prestin per mitjà d'un establiment permanent situat a l'Estat Espanyol.
- I la normativa administrativa corresponent, estatal i autonòmica.

9.15 Conformitat amb la llei aplicable

L'EC-URV manifesta el compliment de la Llei 59/2003, en aquest document, i als instruments jurídics amb subscriptors i verificadors.

9.16 Clàusules diverses

9.16.1 Acord íntegre

L'EC-URV estableix, als seus instruments jurídics vinculants amb els verificadors, clàusules d'acord íntegre.

En virtut de la clàusula d'acord íntegre s'entén que l'instrument jurídic regulador del servei conté la voluntat completa i tots els acords entre les parts.

9.16.2 Subrogació

Els drets i els deures associats a la condició d'Entitat de Certificació no poden ser objecte de cessió a tercers de cap tipus, ni cap tercera entitat no pot subrogar-se en la posició jurídica d'una Entitat de Certificació.

En cas que es produeixi una cessió o subrogació, es procedeix a l'acabament de l'EC-URV.

9.16.3 Divisibilitat

L'EC-URV estableix, els seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules de divisibilitat.

En virtut de la clàusula de divisibilitat, la invalidesa d'una clàusula no afecta la resta del contracte.

En cas que concorri alguna de les causes descrites als articles 7 i 8 de la Llei 7/1998 sobre condicions generals de la contractació, aquestes clàusules es consideren no incorporades al contracte, o nul·les, aquests efectes no determinen la ineficàcia total del contracte, si aquest pot subsistir sense les clàusules indicades.

9.16.4 Aplicacions

Sense estipulació addicional.

9.16.5 Altres clàusules

Sense estipulació addicional.