



**Agència Catalana
de Certificació**

CENTRE DE SUPERCOMPUTACIÓ
DE CATALUNYA



Declaració de Pràctiques de Certificació
Entitat de Certificació Universitats i Recerca


(EC-UR)

Referencia: D1111_E0650_N-DPC EC-UR

Versión: 5.5

Fecha: 30/06/2011

Control documental

Estat formal	Elaborat per: Carlos Alonso – Núria Mombiola (Àrea d'Assessorament)	Aprovat per: Marta Cruellas
Data de creació	30/07/2009	
Control de versions	Data:	30/06/2011
	Descripció:	
Nivell accés informació	pública	
Títol	Declració de Pràctiques de Certificació EC-UR v5r5 cat	
Fitxer	D1111 E0650 N-DPC EC-UR v5r5 cat.pdf	
Control de còpies	Només les còpies disponibles a https://www.catcert.cat/ garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.	
Drets d'autor	 <p>Aquesta obra està subjecta a una llicència Reconeixement-No comercial-Sense obres derivades 2.5 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.</p>	

1. Introducció.....	11
1.1 PRESENTACIÓ	11
1.1.1 Tipus i classes de certificats	11
1.1.2. Relació entre la Declaració de pràctiques de certificació i altres documents .	19
1.2. NOM DEL DOCUMENT I IDENTIFICACIÓ.....	19
1.2.1. Identificació d'aquest document.....	19
1.2.2. Identificació de polítiques de certificació cobertes per aquesta DPC	19
1.3. COMUNITAT D'USUARIS DE CERTIFICATS.....	21
1.3.1. Prestadors de serveis de certificació	22
1.3.2. Entitat de Certificació Arrel	22
1.3.3. EC-UR.....	23
1.3.4. Entitats de Certificació Vinculades.....	23
1.3.5. Entitats de Registre.....	23
1.3.6. Usuaris finals	24
1.4. ÚS DELS CERTIFICATS.....	25
1.4.1. Usos típics dels certificats.....	25
1.4.2. Aplicacions prohibides	35
1.5. ADMINISTRACIÓ DE LA DECLARACIÓ DE PRÀCTIQUES DE CERTIFICACIÓ	37
1.5.1. Organització que administra l'especificació	37
1.5.2. Dades de contacte de l'organització	38
1.5.3. Persona que determina la conformitat d'una DPC amb la política	39
1.5.4. Procediment d'aprovació	39
2. Publicació d'informació i directori de certificats	40
2.1. DIRECTORI DE CERTIFICATS	40
2.2. PUBLICACIÓ D'INFORMACIÓ DE L'EC-UR	40
2.3. FREQUÈNCIA DE PUBLICACIÓ	40
2.4. CONTROL D'ACCÉS	40
3. Identificació i autenticació	41
3.1. GESTIÓ DE NOMS	41
3.1.1. Tipus de noms	41
3.1.2. Significat dels noms	41
3.1.3. Utilització d'anònims i pseudònims	42
3.1.4. Interpretació de formats de noms	42
3.1.5. Unicitat dels noms.....	42
3.1.6. Resolució de conflictes relatius a noms.....	42
3.2. VALIDACIÓ INICIAL DE LA IDENTITAT	43

3.2.1.	Prova de possessió de clau privada	43
3.2.2.	Autenticació de la identitat d'una Organització	44
3.2.3.	Autenticació de la identitat d'una persona física	45
3.2.4.	Informació no verificada	47
3.3.	IDENTIFICACIÓ I AUTENTICACIÓ DE SOL·LICITUDS DE RENOVACIÓ	47
3.3.1.	Validació per a la renovació rutinària de certificats	47
3.3.2.	Validació per a la renovació de certificats després de la revocació	47
4.	Característiques d'operació del cicle de vida dels certificats	48
4.1.	SOL·LICITUD D'EMISSION DE CERTIFICAT	48
4.1.1.	Legitimació per a sol·licitar certificats	48
4.1.2.	Procediment d'alta; Responsabilitats de l'ER	49
4.2.	PROCESSAMENT DE LA SOL·LICITUD DE CERTIFICACIÓ	50
4.2.1.	Certificats personals	50
4.2.2.	Requisits específics per al CEIXSA	51
4.2.3.	Informacions addicionals per al CDS, el CDS-1 EV, el CDSCD i el CDS-1 Seu electrònica EV	52
4.2.4.	Requisits específics per al CIPISR	52
4.2.5.	Altres certificats	52
4.3.	EMISSION DE CERTIFICAT	52
4.3.1.	Accions de l'EC-UR durant el procés d'emissió	52
4.3.2.	Notificació de l'emissió al subscriptor	53
4.4.	ACCEPTACIÓ DEL CERTIFICAT	53
4.4.1.	Responsabilitats de l'Entitat de Registre en el procediment d'alta	53
4.4.2.	Conducta que constitueix acceptació del certificat	54
4.4.3.	Publicació del certificat	55
4.4.4.	Notificació de l'emissió a tercers	55
4.5.	ÚS DEL PARELL DE CLAUS I DEL CERTIFICAT	55
4.5.1.	Ús del parell de claus pels posseïdors de claus i ús del certificat pels subscriptors	55
4.5.2.	Ús pel tercer que confia en certificats	57
4.6.	RENOVACIÓ DE CERTIFICATS SENSE RENOVACIÓ DE CLAUS	57
4.7.	RENOVACIÓ DE CERTIFICATS AMB RENOVACIÓ DE CLAUS	57
4.8.	MODIFICACIÓ DE CERTIFICATS	57
4.9.	REVOCACIÓ I SUSPENSIÓ DE CERTIFICATS	58
4.9.1.	Causas de revocació de certificats	58
4.9.2.	Legitimació per a sol·licitar la revocació	60

4.9.3.	Procediment de sol·licitud de revocació	60
4.9.4.	Període temporal de sol·licitud de revocació	60
4.9.5.	Període màxim de processament de la sol·licitud de revocació	60
4.9.6.	Obligació de consulta d'informació de revocació de certificats.....	61
4.9.7.	Freqüència d'emissió de llistes de revocació de certificats (LRCs)	61
4.9.8.	Període màxim de publicació de LRCs.....	61
4.9.9.	Disponibilitat de serveis de comprovació d'estat de certificats	61
4.9.10.	Obligació de consulta de serveis de comprovació d'estat de certificats	61
4.9.11.	Altres formes d'informació de revocació de certificats	62
4.9.12.	Requisits especials en cas de compromís de la clau privada	62
4.9.13.	Causas de suspensió de certificats.....	62
4.9.14.	Legitimitat per sol·licitar la suspensió.....	63
4.9.15.	Procediments de sol·licitud de suspensió	63
4.9.16.	Període màxim de suspensió	64
4.9.17.	Habilitació d'un certificat suspès	64
4.10.	SERVEIS DE COMPROVACIÓ D'ESTAT DE CERTIFICATS.....	64
4.10.1.	Característiques d'operació dels serveis.....	64
4.10.2.	Disponibilitat dels serveis	64
4.10.3.	Altres funcions dels serveis.....	64
4.11.	ACABAMENT DE LA SUBSCRIPCIÓ	64
4.12.	DIPÒSIT I RECUPERACIÓ DE CLAUS.....	65
4.12.1.	Política i pràctiques de dipòsit i recuperació de claus.....	65
4.12.2.	Política i pràctiques d'encapsulament i recuperació de claus de sessió.....	65
5.	Controls de seguretat física, de gestió i d'operacions.....	66
5.1.	CONTROLS DE SEGURETAT FÍSICA	66
5.1.1.	Localització i construcció de les instal·lacions.....	67
5.1.2.	Accés físic.....	67
5.1.3.	Electricitat i aire condicionat	68
5.1.4.	Exposició a l'aigua	68
5.1.5.	Advertència i protecció d'incendis.....	68
5.1.6.	Emmagatzematge de suports	68
5.1.7.	Tractament de residus	69
5.1.8.	Còpia de seguretat fora de les instal·lacions	69
5.2.	CONTROLS DE PROCEDIMENTS	69
5.2.1.	Funcions fiables	69

5.2.2.	Nombre de persones per tasca.....	70
5.2.3.	Identificació i autenticació per a cada funció	70
5.2.4.	Rols que requereixen separació de tasques.....	70
5.3.	CONTROLS DE PERSONAL	70
5.3.1.	Requisits d'historial, qualificacions, experiència i autorització.....	72
5.3.2.	Requisits de formació	72
5.3.3.	Requisits i freqüència d'actualització formativa	72
5.3.4.	Seqüència i freqüència de rotació laboral.....	72
5.3.5.	Sancions per accions no autoritzades	72
5.3.6.	Requisits de contractació de professionals.....	73
5.3.7.	Subministrament de documentació al personal	73
5.4.	PROCEDIMENTS D'AUDITORIA DE SEURETAT.....	73
5.4.1.	Tipus d'esdeveniments registrats	73
5.4.2.	Freqüència de tractament de registres d'auditoria.....	74
5.4.3.	Període de conservació de registres d'auditoria.....	74
5.4.4.	Protecció dels registres d'auditoria	74
5.4.5.	Procediments de còpies de seguretat.....	74
5.4.6.	Localització del sistema d'acumulació de registres d'auditoria.....	75
5.4.7.	Notificació de l'esdeveniment d'auditoria al causant de l'esdeveniment	75
5.4.8.	Anàlisi de vulnerabilitats	75
5.5.	ARXIU D'INFORMACIONS.....	75
5.5.1.	Tipus d'esdeveniments registrats	76
5.5.2.	Període de conservació de registres	76
5.5.3.	Protecció de l'arxiu.....	76
5.5.4.	Procediments de còpia de suport	76
5.5.5.	Requisits de segellat de cautela de data i hora	77
5.5.6.	Localització del sistema d'arxiu	77
5.5.7.	Procediments d'obtenció i verificació d'informació d'arxiu.....	77
5.6.	RENOVACIÓ DE CLAUS DE LES EC.....	77
5.7.	COMPROMÍS DE CLAUS I RECUPERACIÓ DE DESASTRE	77
5.7.1.	Procediment de gestió d'incidències i compromisos	77
5.7.2.	Corrupció de recursos, aplicacions o dades	77
5.7.3.	Compromís de la clau privada de l'EC-UR	77
5.7.4.	Desastre sobre les instal·lacions	78
5.8.	ACABAMENT DEL SERVEI	78

5.8.1.	EC-UR.....	78
5.8.2.	Entitat de Registre	79
6.	Controls de seguretat tècnica.....	80
6.1.	GENERACIÓ I INSTAL·LACIÓ DEL PARELL DE CLAUS	80
6.1.1.	Generació del parell de claus	80
6.1.2.	Tramesa de la clau privada al subscriptor	81
6.1.3.	Tramesa de la clau pública a l'emissor del certificat.....	81
6.1.4.	Distribució de la clau pública del Prestador de Serveis de Certificació	81
6.1.5.	Mides de les claus	82
6.1.6.	Generació de paràmetres de clau pública	82
6.1.7.	Comprovació de qualitat de paràmetres de clau pública	82
6.1.8.	Generació de les claus en aplicacions informàtiques o en béns d'equip.....	82
6.1.9.	Propòsits d'ús de les claus	82
6.2.	PROTECCIÓ DE LA CLAU PRIVADA	83
6.2.1.	Mòduls de protecció de la clau privada.....	83
6.2.2.	Control per més d'una persona (n de m) sobre la clau privada	83
6.2.3.	Dipòsit de la clau privada.....	83
6.2.4.	Còpia de seguretat de la clau privada	83
6.2.5.	Arxiu de la clau privada.....	84
6.2.6.	Introducció de la clau privada en el mòdul criptogràfic	84
6.2.7.	Emmagatzematge de la clau privada en el mòdul criptogràfic	84
6.2.8.	Mètode d'activació de la clau privada	84
6.2.9.	Mètode de desactivació de la clau privada	84
6.2.10.	Mètode de destrucció de la clau privada.....	84
6.2.11.	Classificació dels mòduls criptogràfics.....	84
6.3.	ALTRES ASPECTES DE GESTIÓ DEL PARELL DE CLAUS.....	85
6.3.1.	Arxiu de la clau pública	85
6.3.2.	Períodes d'utilització de les claus pública i privada	85
6.4.	DADES D'ACTIVACIÓ	85
6.4.1.	Generació i instal·lació de les dades d'activació	85
6.4.2.	Protecció de les dades d'activació.....	85
6.4.3.	Altres aspectes de les dades d'activació	86
6.5.	CONTROLS DE SEGURETAT INFORMÀTICA.....	86
6.5.1.	Requisits tècnics específics de seguretat informàtica	86
6.5.2.	Avaluació del nivell de seguretat informàtica.....	87

6.6.	CONTROLS TÈCNICS DEL CICLE DE VIDA	87
6.6.1.	Controls de desenvolupament de sistemes	87
6.6.2.	Controls de gestió de seguretat	87
6.6.3.	Avaluació del nivell de seguretat del cicle de vida	87
6.7.	CONTROLS DE SEGURETAT DE XARXA	88
6.8.	SEGELL DE TEMPS	88
7.	Perfils de certificats i llistes de certificats revocats	89
7.1.	PERFIL DE CERTIFICAT	89
7.2.	PERFIL DE LA LLISTA DE REVOCACIÓ DE CERTIFICATS	89
8.	Auditoria de conformitat	90
8.1.	FREQÜÈNCIA DE L' AUDITORIA DE CONFORMITAT	90
8.2.	IDENTIFICACIÓ I QUALIFICACIÓ DE L' AUDITOR	90
8.3.	RELACIÓ DE L' AUDITOR AMB L' ENTITAT AUDITADA	90
8.4.	RELACIÓ D' ELEMENTS OBJECTE D' AUDITORIA	90
8.5.	ACCIONS A EMPRENDRE COM A RESULTAT D' UNA FALTA DE CONFORMITAT	90
8.6.	TRACTAMENT DELS INFORMES D' AUDITORIA	91
9.	Requisits comercials i legals	92
9.1.	TARIFES	92
9.1.1.	Tarifa d'emissió o renovació de certificats	92
9.1.2.	Tarifa d'accés a certificats	92
9.1.3.	Tarifa d'accés a informació d'estat de certificat	92
9.1.4.	Tarifes d'altres serveis	92
9.1.5.	Política de reintegrament	92
9.2.	CAPACITAT FINANCERA	92
9.2.1.	Assegurança de responsabilitat civil	92
9.2.2.	Altres actius	92
9.2.3.	Cobertura d'assegurament per a subscriptors i tercers que confien en certificats	92
9.3.	CONFIDENCIALITAT	93
9.3.1.	Informacions confidencials	93
9.3.2.	Informacions no confidencials	93
9.3.3.	Responsabilitat per la protecció d'informació confidencial	93
9.4.	PROTECCIÓ DE DADES PERSONALS	93
9.4.1.	Política de Protecció de Dades Personals	93
9.4.2.	Dades de caràcter personal no disponibles a tercers	95
9.4.3.	Dades de caràcter personal disponibles a tercers	95
9.4.4.	Responsabilitat corresponent a la protecció de les dades personals	96
9.4.5.	Gestió d'incidències relacionades amb les dades de caràcter personal	96

9.4.6.	Prestació del consentiment per al tractament de les dades personals.....	97
9.4.7.	Comunicació de dades personals.....	97
9.5.	DRETS DE PROPIETAT INTEL·LECTUAL.....	98
9.5.1.	Propietat dels certificats i informació de revocació.....	98
9.5.2.	Propietat de la Política de Certificació i la Declaració de Pràctiques de Certificació.....	98
9.5.3.	Propietat de la informació relativa a noms.....	98
9.5.4.	Propietat de claus.....	98
9.6.	OBLIGACIONS I RESPONSABILITAT CIVIL.....	98
9.6.1.	Entitats de Certificació.....	98
9.6.2.	Obligacions i altres compromisos de les Entitats de Registre.....	101
9.6.3.	Garanties ofertes a subscriptors i verificadors.....	102
9.6.4.	Subscriptors.....	103
9.6.5.	Verificadors.....	104
9.6.6.	Altres participants.....	105
9.7.	RENÚNCIES DE GARANTIES.....	105
9.7.1.	Rebuig de garanties de l'EC-UR.....	105
9.8.	LIMITACIONS DE RESPONSABILITAT.....	106
9.8.1.	Limitacions de responsabilitat de l'EC-UR.....	106
9.8.2.	Cas fortuït i força major.....	106
9.9.	INDEMNITZACIONS.....	106
9.9.1.	Clàusula d'indemnitat de subscriptor.....	106
9.9.2.	Clàusula d'indemnitat de verificador.....	106
9.10.	TERMINI I ACABAMENT.....	106
9.10.1.	Termini.....	106
9.10.2.	Finalització.....	106
9.10.3.	Supervivència.....	106
9.11.	NOTIFICACIONS.....	107
9.12.	MODIFICACIONS.....	107
9.12.1.	Procediment per a les modificacions.....	107
9.12.2.	Termini i mecanismes per a notificacions.....	107
9.12.3.	Circumstàncies en les que un OID ha de ser canviat.....	107
9.13.	RESOLUCIÓ DE CONFLICTES.....	108
9.13.1.	Resolució extrajudicial de conflictes.....	108
9.13.2.	Jurisdicció competent.....	108
9.14.	LLEI APLICABLE.....	108

9.15.	CONFORMITAT AMB LA LLEI APLICABLE.....	108
9.16.	CLÀUSULES DIVERSES	108
9.16.1.	Acord íntegre.....	108
9.16.2.	Subrogació	109
9.16.3.	Divisibilitat	109
9.16.4.	Aplicacions	109
9.16.5.	Altres clàusules	109
ANNEX I.....		110
CONTROL DE VERSIONS DPC EC-UR 1R SEMESTRE 2011		110

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 electrònica per incrementar la seguretat de les seves comunicacions telemàtiques.

El 17 de desembre de 2003 es va crear l'Entitat de Certificació Vinculada a la jerarquia d'entitats de certificació de les entitats públiques de Catalunya, anomenada d'Universitats i Recerca (EC-UR), gestionada pel CESCA, en la seva consideració d'Entitat de Certificació Virtual. Aquesta permet a les institucions adherides a l'Anella Científica i a les vinculades amb aquestes obtenir certificats digitals corporatius de classe 1 tant per al seu personal, al seu maquinari o a la mateixa Institució (certificats d'entitat).

En sorgir la necessitat de dotar de signatura electrònica als estudiants, s'amplia l'emissió de certificats amb la inclusió dels certificats d'estudiants que són de classe 2 de col·lectiu.

El conjunt de funcions de col·laboració i suport del CESCA a les institucions en la gestió de les funcions d'emissió tècnica, administració, suspensió, habilitació, revocació i renovació de certificats és el que formen l'Entitat de Registre, també anomenada Entitat de Registre d'Universitats i Recerca (ER-UR). No obstant s'obre la possibilitat que les institucions subscriptores dels certificats de l'Entitat de Certificació i, quan s'escaigui, de les Entitats de Certificació Vinculades a la mateixa, puguin actuar com a Entitat de Registre.

Les institucions actuen com a subscriptores dels certificats i aporten la informació de registre, degudament comprovada, amb la diligència d'una Entitat de Registre Virtual de l'EC-UR o com hem esmentat, realitzen el registre com a Entitat de Registre. També realitzen la validació i l'aprovació interna i prèvia de les sol·licituds de certificats i, quan sigui necessari, sol·liciten la suspensió, habilitació, revocació o renovació de certificats.

A més es regula la possibilitat d'ús, per les entitats de certificació, de nous dispositius criptogràfics amb la consideració de dispositiu segur de creació de signatura electrònica, amb funcionalitats avançades, com l'autenticació amb biometria, i el procediment per a la seva acceptació per l'Entitat de Certificació.

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-UR emetre certificats digitals per a diversos usos i usuaris finals diferents.

Els certificats d'usuaris finals es divideixen en:

- Certificats d'infraestructura, caracteritzats pel fet que el posseïdor de la clau privada és un operador d'una infraestructura, i que s'utilitza per autoritzar operacions relacionades amb els serveis de certificació, com l'aprovació de sol·licituds de certificació.

- 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 (sent en aquest cas el subscriptor o titular del certificat), o en representació i per compte d'una persona jurídica (que serà el subscriptor o titular del certificat).
- 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 (també denominat per a aquests certificats "responsable de custòdia").
- Certificats de dispositiu, caracteritzats pel fet de que el posseïdor de la clau privada és un dispositiu informàtic que realitza operacions de signatura i desxifrat de forma automàtica, sota la responsabilitat d'una persona física o jurídica (denominada subscriptor o titular del certificat).

Els certificats d'usuari final s'emeten en dues modalitats: de classe 1 i de classe 2

Els certificats de classe 1 són certificats corporatius, caracteritzats pel fet que la persona física posseïdora de la clau privada (professor d'universitat, personal d'administració i altres) té una vinculació amb el subscriptor o titular del certificat, que es tracta d'una persona jurídica (una institució). Habitualment, el subscriptor actua com entitat de registre dels certificats mitjançant la certificació administrativa prèvia de les dades, encara que no sigui estrictament necessari.

La resta de certificats són certificats de classe 2 (estudiants, per exemple). El registre de les dades per a l'emissió dels certificats de classe 2 el realitza sempre l'Entitat de Certificació o una entitat de Registre sota la responsabilitat de l'Entitat de Certificació, mitjançant la certificació administrativa prèvia de les dades, quan l'emissió es produeixi a un públic restringit, o mitjançant la captació directa de tota la informació necessària per a l'emissió dels certificats.

L'Entitat de Certificació podrà emetre els següents tipus de certificats:

1.1.1.1 Certificats d'infraestructura

- Certificat d'infraestructura personals d'identificació i signatura electrònica reconeguda d'operadors (CIPISR), que s'empra per autoritzar operacions relacionades amb els serveis de certificació, com l'aprovació de sol·licituds de certificació.
- Certificat d'infraestructura d'entitat de certificació vinculada (CIC), que s'expedeix a les entitats de certificació de les institucions, amb nivell 3, ja que l'Entitat que els signa és de nivell 2.
- Certificat d'infraestructura de dispositiu servidor segur (CIDS), que és utilitzat per una aplicació informàtica servidor de SSL o de TLS d'infraestructura per identificar-se davant les aplicacions client que s'hi connecten i per protegir el secret de les comunicacions entre el client i el servidor, com per exemple els servidors de les entitats de certificació.
- Certificat d'infraestructura de dispositiu d'aplicació digitalment assegurada (CIDA), que és utilitzat per aplicacions informàtiques de la infraestructura que s'identifiquen digitalment, signen electrònicament webservices o altres protocols i que reben documents i missatges xifrats, com per exemple les aplicacions de notificació de missatges de les entitats de certificació.

- Certificat d'infraestructura de servidor d'estat de certificats en línia (CIO), que és utilitzat per un servidor *OCSP Responder* per signar les seves respostes sobre l'estat de validesa dels certificats.
- Certificat d'infraestructura d'entitat de segells de temps (CIT), que és utilitzat per una entitat per signar els segells de temps que emet.
- Certificat d'infraestructura d'entitat de validació (CIV), que és utilitzat per un servidor d'entitat de validació per signar els seus informes.

1.1.1.2. Certificats personals

L'EC-UR emet els següents tipus de certificats personals:

- Certificats personals d'identificació 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 signatura, així com missatges d'autenticació i d'accés segur a sistemes informàtics.
- Certificats personals d'identificació i de signatura electrònica reconeguda de classe 1 amb càrrec per a estrangers (CPISR-1 amb Càrrec Estranger), que identifiquen a la persona que els posseeix, la seva organització subscriptora, i el seu càrrec en aquesta, i que serveixen per a signar missatges amb dispositiu segur de creació de signatura, així com missatges d'autenticació i d'accés segur a sistemes informàtics
- Certificats personals d'identificació i signatura electrònica reconeguda de classe 1 amb càrrec per a ús concret (CPISR-1 amb Càrrec ús), que identifiquen la persona que els posseeix, la seva organització subscriptora, el seu càrrec en aquesta, i les limitacions materials d'ús, i que serveixen per signar missatges amb dispositiu segur de creació de signatura, així com missatges d'autenticació i d'accés segur a sistemes informàtics.
- Certificats personals de xifrat de classe 1 amb càrrec (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 o produir missatges confidencials.
- Certificats personals de xifrat de classe 1 amb càrrec per a estrangers (CPX-1 amb Càrrec Estranger), que identifiquen a la persona que els posseeix, la seva organització subscriptora, i el seu càrrec en aquesta, i que s'utilitzen per a rebre o produir missatges confidencials.
- Certificats personals de xifrat de classe 2 amb càrrec (CPX-2 Càrrec), que identifiquen la persona que els posseeix, la seva organització subscriptora, i el seu càrrec en aquesta, i que s'utilitzen per rebre o produir missatges confidencials
- Certificats personals d'identificació i de signatura electrònica reconeguda de classe 2 amb càrrec (CPISR-2 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 signatura, així com missatges d'autenticació i d'accés segur a sistemes informàtics.
- Certificats personals d'identificació 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 signatura, així com missatges d'autenticació i d'accés segur a sistemes informàtics.

- Certificats personals d'identificació i de signatura electrònica reconeguda de classe 2 per a estudiants estrangers (CPISR-2 d'Estudiant Estranger), que identifiquen a la persona que els posseeix, la seva organització subscriptora, i la seva condició d'estudiant, i que serveixen per a signar missatges amb dispositiu segur de creació de signatura, així com missatges d'autenticació i d'accés segur a sistemes informàtics.
- Certificats personals de xifrat de classe 2 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 o produir missatges confidencials.
- Certificats personals de xifrat de classe 2 per estudiants estrangers (CPX-2 d'Estudiant Estranger), que identifiquen a la persona que els posseeix, la seva organització subscriptora, i la seva condició d'estudiant, i que s'utilitzen per a rebre, i produir missatges confidencials.
- Certificats personals d'identificació, xifrat i signatura avançada amb càrrec d'empleat públic de classe 1 (CPIXSA-1 Càrrec EP), que identifiquen la persona que els posseeix, la seva organització subscriptora, i que serveixen per signar missatges d'autenticació i d'accés segur a sistemes informàtics.

El certificat d'identificació i de signatura electrònica reconeguda de classe 1 amb càrrec (CPISR-1 Càrrec), el certificat personal d'identificació i signatura reconeguda de classe 1 amb càrrec per a estrangers (CPISR-1 amb Càrrec Estranger), i el certificat d'identificació i de signatura electrònica reconeguda de classe 1 amb càrrec per a ús concret (CPISR-1 Càrrec ús) són certificats reconeguts 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 emesos complint les obligacions dels articles 12, 13, 18 i 20 de la Llei esmentada. Funcionen amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. 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, 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 cap compliment de requisit addicional. A més inclouen una manifestació relativa a la categoria de personal i/o 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 comprova les facultats i poders de signatura del posseïdor mitjançant altres mitjans, diferents del certificat. També es poden utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura manuscrita, sinó només la identificació del posseïdor de claus.

El certificat personal de xifrat de classe 1 amb càrrec (CPX-1 Càrrec), el certificat personal de xifrat de classe 1 amb càrrec per a estrangers (CPX-1 amb Càrrec Estranger) i el certificat personal de xifrat de classe 2 amb càrrec (CPX-2 càrrec), són certificats reconeguts de conformitat amb el que s'estableix a l'article 6 i 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. Funcionen amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de

desembre, i que compleixen allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. Garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten xifrar documents i rebre missatges de dades confidencials, en qualsevol format.

El certificat d'identificació i de signatura electrònica reconeguda de classe 2 amb càrrec (CPISR-2 Càrrec) 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 signatura, 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, 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 cap compliment de requisit addicional. A més, inclou una manifestació relativa 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 comprova 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 manuscrita, sinó només la identificació del posseïdor de claus.

El certificat personal d'identificació i de signatura electrònica reconeguda de classe 2 per estudiants (CPISR-2 d'Estudiant), i el certificat personal d'identificació i de signatura electrònica reconeguda de classe 2 per a estudiants estrangers (CPISR-2 d'Estudiant Estranger), són certificats reconeguts 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. Funcionen amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i donen compliment a allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. 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, 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 cap compliment de requisit addicional. A més inclouen 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. 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 comprova les facultats i poders de signatura del posseïdor mitjançant altres mitjans, diferents del certificat. També es poden utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura manuscrita, sinó només la identificació del posseïdor de claus.

El certificat personal de xifrat de classe 2 per a estudiant (CPX-2 d'Estudiant), i el certificat personal de xifrat per a estudiant estranger (CPX-2 d'Estudiant Estranger), són certificats reconeguts de conformitat amb el que s'estableix a l'article 6 i 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. Funcionen amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i que compleixen allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. Garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten xifrar documents i rebre missatges de dades confidencials, en qualsevol format.

El certificat personal de xifrat de classe 2 amb càrrec (CPX-2 càrrec) és un certificat reconegut de conformitat amb el que s'estableix a l'article 6 i 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. 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 compleix allò 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 signatura, i permet xifrar documents i rebre missatges de dades confidencials, en qualsevol format.

El certificat personal d'identificació, xifrat i signatura avançada amb càrrec d'empleat públic de classe 1 (CPIXSA-1 Càrrec EP) és un certificat reconegut de conformitat amb el que s'estableix a l'article 6 i 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. Garanteix la identitat del subscriptor i el posseïdor de la clau privada d'identificació i signatura, i permet la generació de la "signatura electrònica avançada".

A més, en funció dels requisits tècnics i de les necessitats dels usuaris, és 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 d'entitat

L'EC-UR emet els següents tipus de certificats d'entitat:

- Certificats d'entitat d'identificació amb signatura electrònica reconeguda de classe 1 (CEISR-1), d'acord amb l'establert en l'article 7 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, que permeten que Institucions públiques i privades, corporacions de dret públic i persones jurídic-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 de classe 1 (CEX-1), d'acord amb l'establert en l'article 7 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, que permeten que Institucions públiques i privades, corporacions de dret públic i persones jurídic-públiques (col·lectivament anomenades "entitats") puguin produir i rebre documents confidencials.
- Certificats d'entitat d'identificació, xifrat i signatura electrònica avançada (CEIXSA) d'acord amb l'establert en l'article 7 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, que permeten que Institucions públiques i privades, corporacions de dret públic i persones jurídic-públiques (col·lectivament denominades "entitats") signin documents electrònicament, missatges d'autenticació

(confirmació de la identitat) i d'accés segur a sistemes informàtics i puguin produir i rebre documents confidencials.

Adicionalment, 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.

1.1.1.4. Certificats de dispositiu

L'EC-UR emet els següents tipus de certificats de dispositiu:

- Certificat de dispositiu servidor segur de classe 1 (CDS-1), 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 servidor segur de classe 1 Extended Validation (CDS-1 EV), 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, tot oferint la validació automàtica al navegador.
- Certificat de dispositiu de seu electrònica nivell mig de classe 1 Extended Validation (CDS-1 SENM EV), que serveix per identificar i garantir una comunicació segura amb la seu electrònica d'un ens, entenent seu electrònica en els termes que la descriu l'article 10 de la Llei 11/2007, d'accés electrònic dels ciutadans als serveis públics.

Aquest certificat es pot utilitzar per a la connexió segura dels ciutadans a pàgines web oficials, l'autenticació d'un lloc web, l'allotjament de registres electrònics, la consulta i autorització de registres de representació, etc.

El certificat de nivell mig, amb unes claus de 1024 bits, és recomanable per a la majoria de les administracions públiques que poden tenir els següents riscos: infracció de seguretat (p.e. robatori de la identitat), pèrdues econòmiques moderades, pèrdua d'informació sensible o crítica o refutació d'una transacció amb impacte econòmic significatiu.

- Certificat de dispositiu de seu electrònica nivell alt de classe 1 Extended Validation (CDS-1 SENA EV), que serveix per identificar i garantir una comunicació segura amb la seu electrònica d'un ens, entenent seu electrònica en els termes que la descriu l'article 10 de la Llei 11/2007, d'accés electrònic dels ciutadans als serveis públics.

Aquest certificat pot utilitzar-se per a la connexió segura dels ciutadans a pàgines web oficials, l'autenticació d'un lloc web, l'allotjament de registres electrònics, la consulta i autorització de registres de representació, etc.

El certificat de nivell alt, amb unes claus de 2048 bits, és recomanable per a aquelles administracions públiques que, havent realitzat prèviament una anàlisi de riscos, precisen mesures addicionals de seguretat, doncs contempen els següents riscos: infracció de seguretat, pèrdues econòmiques importants, pèrdua d'informació altament sensible i crítica o refutació d'una transacció amb impacte econòmic molt significatiu.

- El certificat de nivell alt s'haurà d'emmagatzemar en un HSM (maquinari criptogràfic).
- Certificat de dispositiu segur de controlador de domini de classe 1 (CDSCD-1), s'utilitza per una aplicació informàtica, servidor SSL o TLS, per a 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 de classe 1 (CDA-1), que és utilitzat per aplicacions informàtiques que s'identifiquen digitalment, signen electrònicament webservices o altres protocols i que rebin documents i missatges xifrats.
- Certificat de dispositiu de segell electrònic de Administració, òrgan o entitat de dret públic nivell mig de classe 1 (CDA-1 segell electrònic nivell mig), és un certificat digital que serveix per a la identificació i l'autenticació de l'exercici de la competència en l'actuació administrativa automatitzada, en els termes descrits en l'article 18 de la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics. Aquest certificat es pot utilitzar per a l'intercanvi de dades entre administracions, la identificació i autenticació d'un sistema, servei web o aplicació, l'arxiu electrònic automatitzat, les compulses i còpies electròniques, entre d'altres.
- El certificat de nivell mig, amb unes claus de 1024 bits, és recomanable per a la majoria de les administracions públiques que poden tenir els següents riscos: infracció de seguretat (p.e. robatori de la identitat), pèrdues econòmiques moderades, pèrdua d'informació sensible o crítica o refutació d'una transacció amb impacte econòmic significatiu.
- Certificat de dispositiu de segell electrònic de Administració, òrgan o entitat de dret públic nivell alt de classe 1 (CDA-1 segell electrònic nivell alt), serveix per a la identificació i l'autenticació de l'exercici de la competència en l'actuació administrativa automatitzada, en els termes descrits en l'article 18 de la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics.
- Aquest certificat es pot utilitzar per a l'intercanvi de dades entre administracions, la identificació i autenticació d'un sistema, servei web o aplicació, l'arxiu electrònic automatitzat, les compulses i còpies electròniques, entre d'altres.
- El certificat de nivell alt, amb unes claus de 2048 bits, és recomanable per a aquelles administracions públiques que, havent realitzat prèviament una anàlisi de riscos, precisen mesures addicionals de seguretat, doncs contempen els següents riscos: infracció de seguretat, pèrdues econòmiques importants, pèrdua d'informació altament sensible i crítica o refutació d'una transacció amb impacte econòmic molt significatiu.
- El certificat de segell electrònic de nivell alt es carregarà directament a la PSIS (Plataforma de serveis d'identificació i signatura), almenys mentre no es disposi del maquinari criptogràfic HSM necessari per al nivell de seguretat requerit.
- Certificat de dispositiu de signatura d'aplicacions informàtiques de classe 1 (CDP-1), que serveix per signar digitalment aplicacions informàtiques a transmetre per mitjà 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-UR.

L'EC-UR 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, que inclou els procediments que aplica l'EC-UR 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-UR".

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

1.3.6.1.4.1.15096.1.2.7

1.2.2.Identificació de polítiques de certificació cobertes per aquesta DPC

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

- **CIPISR** – Certificat d'infraestructura d'operador, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.15
Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.16
- **CIC** – Certificat d'infraestructura d'Entitat de Certificació Vinculada, emès per l'EC-UR
CIC-1. OID: 1.3.6.1.4.1.15096.1.3.1.11
CIC-2. OID: 1.3.6.1.1.4.15096.1.3.1.12
CIC-3. OID: 1.3.6.1.4.1.15096.1.3.1.13
- **CIDS-1** – Certificat d'infraestructura de servidor segur, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.17
- **CIDA-1** – Certificat d'infraestructura d'aplicació, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.18
- **CIO-1** – Certificat d'infraestructura de servidor d'estat de certificats en línia, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.19

- **CIV-1** – Certificat d'infraestructura d'entitat de validació, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.20
- **CIT-1** - Certificat d'infraestructura d'entitat de segells de temps, emès per l'EC-UR
Classe 1. 1.3.6.1.4.1.15096.1.3.1.111
- **CPISR-1 Càrrec** - Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.2.1
- **CPISR-1 amb Càrrec Estranger** – Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec per a estrangers, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.1.1
- **CPISR-1 amb Càrrec Ús** - Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec per a ús concret, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.3.3
- **CPX Càrrec** - Certificat personal de xifrat amb càrrec, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.41.1.1
Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.42.3.1
- **CPX-1 amb Càrrec Estranger** – Certificat personal de xifrat amb càrrec per a estrangers, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.41.2.1
- **CPISR-2 amb Càrrec** – Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec, emès per l'EC-UR
Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.82.3.1
- **CPISR-2 d'Estudiant** - Certificat personal d'identificació i signatura electrònica reconeguda, d'estudiant, emès per l'EC-UR
Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.82.2.1
- **CPISR-2 d'Estudiant Estranger** - Certificat personal d'identificació i signatura electrònica reconeguda per a estudiants estrangers, emès per l'EC-UR
Classe 2. OID: 1.3.6.1.4.1.15096. 1.3.1.82.2.3
- **CPX-2 d'Estudiant** - Certificat personal de xifrat d'estudiant, emès per l'EC-UR
Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.42.2.1
- **CPX-2 d'Estudiant Estranger** - Certificat personal de xifrat d'estudiant estranger, emès per l'EC-UR
Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.42.2.3
- **CPIXSA-1 Càrrec EP** – Certificat personal d'identificació, xifrat i signatura electrònica avançada amb càrrec d'empleat públic, emès per l'EC-UR
OID: 1.3.6.1.4.1.15096.1.3.1.85

- **CEISR-1** – Certificat d'entitat d'identificació amb signatura electrònica reconeguda, emès per l'EC-UR.
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.121.3
- **CEX-1** – Certificat d'entitat de xifrat emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.131.3
- **CEIXSA-1** – Certificats d'entitat d'identificació, xifrat i signatura electrònica avançada emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.161.3
- **CDS-1** - Certificat de dispositiu servidor segur, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51
- **CDS-1 EV**- Certificat de dispositiu servidor segur Extended Validation, emès per l'EC-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.4
- **CDS-1 SENM EV**– Certificat de dispositiu servidor segur, seu electrònica nivell mig Extended Validation, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.2
- **CDS-1 SENA EV**– Certificat de dispositiu servidor segur, seu electrònica nivell alt Extended Validation, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.3
- **CDA-1** - Certificat de dispositiu d'aplicació digitalment assegurada, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.91
- **CDA-1 SENM** - Certificat de dispositiu d'aplicació digitalment assegurada, segell electrònic nivell mig, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.91.1
- **CDA-1 SENA** - Certificat de dispositiu d'aplicació digitalment assegurada, segell electrònic nivell alt, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.91.2
- **CDP-1** - Certificat de dispositiu de signatura de programari, emès per l'EC-UR
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.71
- **CDSCD-1** - certificat de dispositiu segur de controlador de domini, emès per l'EC-UR.
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-UR no s'expedeixen al públic, sinó a les entitats, al personal, als estudiants i als dispositius de les universitats, els centres de recerca i altres institucions de Catalunya, en el seu cas, adherides a l'"Anella Científica" o vinculades amb aquestes (d'ara endavant, "les institucions").

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 signen els certificats.

En el sistema públic català de certificació, podran oferir serveis els prestadors següents:

- 1) Prestadors de serveis de certificació de les institucions
- 2) Prestadors classificats per CATCert com a serveis de certificació

1.3.1.1. Prestadors de serveis de certificació de les institucions

CATCert serà el prestador de serveis de certificació de l'Entitat de Certificació, amb la corresponent Autoritat de Certificació diferenciada i vinculada a la jerarquia pública de certificació de Catalunya.

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

1.3.1.2. Prestadors de serveis de certificació classificats

Els prestadors de serveis de certificació, públics o privats, diferents de les institucions, que operin en el mercat d'acord amb la Llei 59/2003, de 19 de desembre, de signatura electrònica, podran sol·licitar a CATCert la seva classificació, a efectes del reconeixement i l'ús dels seus certificats per part de les institucions.

Les condicions de classificació i els mecanismes tècnics per a l'ús dels certificats de proveïdors classificats per part de les institucions seran prèviament establerts per CATCert.

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" (<http://www.catcert.cat/descarrega/acc.crt>), i 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 electrònica 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 les Institucions.

1.3.4. Entitats de Certificació Vinculades

Les institucions són Entitats de Certificació Vinculades a l'EC-UR quan realitzen els serveis d'expedició i gestió dels certificats i es troben inscrites en la jerarquia pública de certificació de Catalunya, dins de la comunitat d'usuaris certificats de l'Entitat de Certificació.

Amb una Entitat de Certificació Vinculada, la institució emet certificats a usuaris finals, de tipus personal, d'entitat o de dispositius.

Quan la institució delega a CATCert l'operació de l'entitat de certificació vinculada, en la seva qualitat legal de prestador de serveis de certificació, la institució roman responsable de l'organització i les decisions de gestió referides a l'entitat de certificació. Aquest funció, que no pot ser objecte de delegació, s'anomena Entitat de Certificació Virtual.

1.3.5. Entitats de Registre

Les Entitats de Registre són persones físiques o jurídiques que assisteixen a les Entitats de Certificació Vinculades 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.

El procés de creació d'entitats de registre és responsabilitat de l'administrador de l'Entitat de Certificació. Mitjançant acord o conveni es constitueix l'entitat de registre. CATCert verifica que l'Entitat de Registre compti amb els recursos materials i humans necessaris, i de la designació del personal responsable. Tanmateix, és responsable, en tot cas, de la formació del personal que emeti els certificats com a operadors de l'entitat de registre i, a tal efecte, de l'emissió dels certificats d'operador corresponents (típicament, CIPISR). CATCert validarà les peticions de certificats de les Entitats de Registre examinant la sol·licitud i fent les comprovacions necessàries per al compliment de la Política General de Certificació i de la Declaració de Pràctiques de Certificació.

En certificats de classe 1 i en certificats corporatius o col·lectius de qualsevol classe, l'Entitat de Registre i el subscriptor podran ser la mateixa organització. Habitualment, l'Entitat de Registre podrà actuar com a sol·licitant del certificat.

En certificats de classe 2, l'Entitat de Registre i el subscriptor hauran de ser necessàriament organitzacions diferents, doncs l'Entitat de Registre ha d'actuar sempre per compte de l'Entitat de Certificació Vinculada.

El CESCA actuarà, en tot cas, com Entitat de Registre per a totes les institucions subscriptores de certificats de classe 1 que no es constitueixin com Entitat de Registre. En

aquest cas, han d'aportar les necessàries dades personals i corporatives, legalment certificades, per l'emissió de certificats.

1.3.6. Usuaris finals

Els usuaris finals són les persones que obtenen i utilitzen certificats emesos per l'Entitat de Certificació, i, en concret, podem distingir els següents usuaris finals:

- a) Els sol·licitants de certificats
- b) Els subscriptors o titulars de certificats
- c) Els posseïdors de claus
- d) Els verificadors de signatures, de segells i de certificats

1.3.6.1. Sol·licitants de certificats

Tot certificat ha de ser sol·licitat per una persona, en el seu propi nom, en nom d'una institució o en nom d'una altra persona física o jurídica.

Poden ser sol·licitants:

- a) La persona que serà el futur posseïdor de claus o el futur subscriptor del certificat
- b) Una persona autoritzada pel futur subscriptor
- c) Una persona autoritzada per l'Entitat de Registre
- d) Una persona autoritzada per l'Entitat de Certificació

L'autorització podrà realitzar-se tant de forma expressa com tàcita, i en aquells casos en els quals l'entitat de certificació ho consideri convenient haurà de formalitzar-se documentalment.

1.3.6.2. Subscriptors de certificats

Els subscriptors són les institucions i les persones, físiques o jurídiques, així identificats al camp "Subject" del certificat.

En certificats de dispositiu, al camp "Subject" també s'identifica el dispositiu.

El subscriptor té llicència d'ús del certificat i, quan es tracta d'una institució o una altra persona jurídica, i el certificat és personal, actua sempre a través d'un posseïdor de claus, degudament autoritzat, i que figura identificat al certificat.

1.3.6.3. Posseïdors de claus

Els posseïdors de claus són les persones físiques que posseeixen de forma exclusiva les claus de signatura digital de certificats CPISR de classe 1 o de classe 2 col·lectiu, es troben degudament autoritzats per a això pel subscriptor i degudament identificats al certificat mitjançant el seu nom i cognoms.

També existeixen posseïdors de claus de xifrat, en certificats CPX, amb la peculiaritat que la clau de desxifrat, a diferència de la clau de signatura, pot ser recuperada, en certs casos i condicions, per l'Entitat de Certificació corresponent.

Típicament, seran posseïdors de claus dels certificats de classe 1 d'una institució universitària, el personal al seu servei, incloent-hi professors i personal d'administració. Els Estudiants de la Institució seran posseïdors de claus dels certificats de classe 2.

1.3.6.4. Usuaris de certificats

Els usuaris dels certificats són els verificadors.

1.3.6.5. Verificadors de certificats

Els verificadors són les persones físiques i jurídiques que reben signatures electròniques, segells electrònics i certificats digitals i han de verificar-los, com pas previ a confiar-hi.

Per exemple, seran verificadors de certificats la resta d'institucions universitàries i de recerca, les administracions públiques i, en general, les persones físiques i jurídiques amb les que es pugui relacionar el posseïdor de claus.

Els verificadors, tot i que sempre poden confiar absolutament en la identitat del posseïdor de claus i en la seva relació amb la institució subscriptora del seu certificat, han de practicar altres comprovacions addicionals si volen confiar en l'acte jurídic del qual es dona prova al document o missatge signat pel posseïdor.

Per exemple, és necessari comprovar que un posseïdor sense un càrrec concret està facultat legalment, o mitjançant una previsió estatutària o un apoderament o habilitació concrets, abans de confiar en l'acte documentat, ja que el certificat no aporta aquesta garantia.

En canvi, sí es pot confiar sempre en el càrrec, de forma que tot el que pot fer, per exemple el rector, mitjançant un document en suport paper, per escrit, també ho pot fer electrònicament, sense que sigui necessària cap comprovació addicional.

1.4. Ús dels certificats

Aquesta secció llista les aplicacions en les quals es pot utilitzar cada tipus de certificat, estableix limitacions i prohibeix algunes aplicacions dels certificats.

1.4.1. Usos típics dels certificats

1.4.1.1. Certificats d'infraestructura

1.4.1.1.1. Requisits específics per al Certificat Personal d'Infraestructura d'Identificació i Signatura Reconeguda (CIPISR)

Els certificats personals d'infraestructura d'identificació i signatura reconeguda (CIPISR) són emesos a operadors d'Entitats de Registre, per als treballs d'emissió i gestió del cicle de vida de certificats d'una Entitat de Certificació.

Els certificats d'infraestructura d'identificació i signatura són certificats reconeguts d'acord amb el que s'estableix a l'article 11.1, amb el contingut prescrit per l'article 11.2 i emesos complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

Els CIPIR funcionen amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i que donen compliment a allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Per aquest motiu, els CIPIR garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten la generació de la "signatura electrònica reconeguda"; és a dir, la signatura electrònica avançada que es basa en un certificat reconegut i que ha estat generada emprant un dispositiu segur, per la qual cosa, d'acord amb el que estableix l'article 3 de la Llei 59/2003, de 19 de desembre, s'equipara a la signatura escrita per efecte legal, sense necessitat de complir cap altre requeriment addicional.

Els CIPIR són certificats d'operador i el seu ús exclusiu és l'operació dels components de la infraestructura de clau pública de CATCert com, per exemple, els components emprats per les Entitats de Registre per aprovar i generar certificats, o per revocar-los, o pel servei d'atenció a usuaris per suspendre certificats.

Els CIPIR corresponents a l'Entitat de Certificació seran emesos per la pròpia Entitat de Certificació, amb l'aprovació prèvia de CATCert.

Els CIPIR corresponents a cada Entitat de Certificació Vinculada a l'Entitat de Certificació seran emesos per la pròpia Entitat de certificació, amb l'aprovació prèvia de l'Entitat de Certificació.

1.4.1.1.2. Requisits específics per al CIC

Els certificats d'entitat de certificació (CIC) són emesos per l'Entitat de Certificació Arrel, a organitzacions que operen una Entitat de Certificació dins de la seva jerarquia, per a diferents usos, segons la seva classe:

- Signatura de peticions de renovació, suspensió i revocació de certificats CIC
- Emissió i signatura de certificats CIC, CIDS, CIDA, CIO, CIV, CIT, CIPIR, CPX, CEX, CDS-1 i CDA-1.
- Emissió i signatura de llistes de revocació de certificats (LRC).

Els CIC s'obtenen després d'un procés d'admissió de l'Entitat de Certificació Vinculada als serveis de certificació de l'Agència Catalana de Certificació, que es descriu en la declaració de pràctiques de certificació (DPC) de l'entitat de certificació arrel de la jerarquia.

1.4.1.1.3. Requisits específics per al CIDS

Els certificats d'infraestructura de dispositiu servidor segur (CIDS) s'emeten a Entitats de Certificació, 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

Els certificats CIDS són certificats ordinaris, i que garanteixen la identitat de l'Entitat de Certificació i del servidor concret on funcionen.

1.4.1.1.4. Requisits específics per al CIDA

Els certificats d'infraestructura de dispositiu d'aplicació digitalment assegurada (CIDA) s'emeten a Entitats de Certificació responsables de l'operació d'aplicacions informàtiques que s'identifiquen digitalment, signen electrònicament *webservices* o altres protocols i que reben documents i missatges xifrats.

Els certificats CIDA són certificats ordinaris, que garanteixen la identitat de l'Entitat de Certificació i la integritat i l'autenticitat de les dades signades. També permeten la recepció d'informació xifrada.

La clau privada del CIDA podrà estar arxivada per l'entitat de certificació de manera que, en certes circumstàncies, pugui recuperar-se i accedir a la informació xifrada, sota demanda de l'Entitat de Certificació.

1.4.1.1.5. Requisits específics per al CIO

Els certificats d'infraestructura de servidor d'estat de certificats en línia (CIO) s'emeten a Entitats de Certificació, responsables de l'operació d'un servidor *OCSP Responder* per signar les seves respostes sobre l'estat de validesa dels certificats.

Els certificats CIO són certificats ordinaris, que garanteixen la identitat de l'Entitat de Certificació i del servidor *OCSP Responder* i la integritat i l'autenticitat de les dades signades.

1.4.1.1.6. Requisits específics per al CIT

Els certificats d'infraestructura d'entitat de segells de temps (CIT) s'emeten a Entitats de Certificació, responsables de l'operació d'un servidor per signar els segells de temps que emet.

Els certificats CIT són certificats ordinaris, que garanteixen la identitat de l'Entitat de Certificació i del servidor de signatura de segells de temps i la integritat i l'autenticitat de les dades signades.

1.4.1.1.7. Requisits específics per al CIV

Els certificats d'infraestructura d'entitat de validació (CIV) s'emeten a Entitats de Certificació, responsables de l'operació d'un servidor d'entitat de validació per signar els seus informes.

Els certificats CIV són certificats ordinaris, que garanteixen la identitat de l'Entitat de Certificació i del servidor d'entitat de validació i la integritat i l'autenticitat de les dades signades.

1.4.1.2. Certificats personals

1.4.1.2.1. Certificats personals d'identificació i signatura electrònica reconeguda de classe 1 amb càrrec (CPISR-1 càrrec), i amb càrrec per a estrangers (CPISR-1 càrrec estrangers), i Certificats personals d'identificació i signatura electrònica reconeguda de classe 1 amb càrrec per a ús concret (CPISR-1 càrrec ús).

Els certificats personals d'identificació i signatura reconeguda de classe 1 amb càrrec, i amb càrrec per a estrangers, i els Certificats personals d'identificació i signatura electrònica reconeguda de classe 1 amb càrrec per a ús concret 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 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 categoria de personal i/o càrrec del posseïdor de claus, que han estat comprovats abans d'emetre el certificat, i són correctes, d'acord amb aquesta Declaració de pràctiques.

El Certificat personal d'identificació i signatura electrònica reconeguda de classe 1 amb càrrec per a ús concret identifica, a més de la persona que els posseeix, la seva organització subscriptora, i el seu càrrec en aquesta, les limitacions materials d'ús.

A més, els tres certificats 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.

1.4.1.2.2. Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec (CPISR-2 càrrec)

El certificat personal d'identificació i signatura reconeguda de classe 2 amb càrrec és un certificat reconegut 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.

Es tracta d'un certificat reconegut que 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.

Per aquest motiu, aquest certificat garanteix la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, 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, 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.

Aquest certificat inclou una manifestació relativa al càrrec del posseïdor de claus, que ha estat comprovat abans d'emetre el certificat, i és correcte i vigent mentre el certificat també es troba vigent.

A més, es pot 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.

1.4.1.2.3. Certificats personals d'identificació i signatura electrònica reconeguda de classe 2 d'estudiant (CPISR-2 estudiant), i d'estudiant estranger (CPISR-2 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 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 manuscrita 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 ha estat comprovada abans d'emetre el certificat, i és correcta i vigent 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.

1.4.1.2.4. Certificats personals de xifrat de classe 1 amb càrrec (CPX-1 càrrec), i amb càrrec per a estrangers (CPX-1 amb càrrec estranger)

El certificat personal de xifrat de classe 1 amb càrrec i el certificat personal de xifrat de classe 1 amb càrrec per a 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 emesos complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Es tracta de 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.

Els certificats personals de xifrat s'utilitzen exclusivament per a xifrar documents i rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, per part del remitent del missatge.

Aquests certificats garanteixen la identitat del subscriptor, però no permeten la signatura electrònica de missatges de dades.

La clau privada d'aquests certificats està 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.

1.4.1.2.5. Certificats personals de xifrat de classe 2 amb càrrec (CPX-2 càrrec)

El certificat personal de xifrat de classe 2 amb càrrec és un certificat reconegut 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 donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Es tracta d'un certificat reconegut que 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.

Els certificats personals de xifrat amb càrrec s'utilitzen exclusivament per xifrar documents i rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, per part del remitent del 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 forma que, en determinades circumstàncies, pugui recuperar-se i accedir a la informació xifrada, inclòs sense la intervenció del subscriptor o del posseïdor de claus.

1.4.1.2.6. Certificats personals de xifrat de classe 2 d'estudiant (CPX-2 estudiant), i d'estudiant estranger (CPX-2 d'estudiant estranger)

El certificat personal de xifrat de classe 2 per a estudiants i el certificat personal de xifrat de classe 2 per a estudiants 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 emesos complint les

obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Es tracta de 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.

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

Aquests certificats garanteixen la identitat del subscriptor, però no permeten la signatura electrònica de missatges de dades.

La clau privada d'aquests certificats està 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.

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.

1.4.1.2.7. Certificats personals d'identificació, xifrat i signatura avançada amb càrrec d'empleat públic de classe 1 (CPIXSA-1 Càrrec EP)

El certificat personal d'identificació, xifrat i signatura avançada amb càrrec d'empleat públic de classe 1 és un certificat reconegut 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.

S'utilitza per a signar sense dispositiu segur de creació de signatura, donant suport a la signatura electrònica avançada segons l'article 3.2 de la Llei 59/2003, de 19 de desembre.

Aquests certificats poden incloure una manifestació relativa al càrrec del posseïdor de claus, que ha estat comprovat abans d'emetre el certificat, i és correcta i vigent mentre el certificat també es troba vigent.

El Certificat personal d'identificació, xifrat i signatura electrònica avançada amb càrrec d'empleat públic de classe 1, a més de la persona que els posseeix, la seva organització subscriptora, i el seu càrrec en aquesta, les limitacions materials d'ús.

A més es pot 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 d'Entitat

1.4.1.3.1. Certificats d'Entitat d'Identificació amb Signatura Electrònica Reconeguda de classe 1 (CEISR-1)

Els certificats d'entitat d'identificació amb signatura reconeguda de classe 1 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 signatura electrònica, i 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 de signatura, essent idonis per a oferir suport a la signatura electrònica reconeguda de l'entitat; és a dir, és 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 3.4 de la Llei 59/2003, de 19 de desembre, s'equipara a la signatura manuscrita per efecte legal, sense necessitat de complir cap altre requeriment addicional.

1.4.1.3.2. Certificat d'Entitat de Xifrat de classe 1 (CEX-1)

Els certificats d'entitat de xifrat de classe 1 són certificats reconeguts, no emesos al públic, que s'expedeixen a subscriptors i s'utilitzen exclusivament per xifrar documents o rebre missatges 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 expedit 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. La clau privada del CEX s'arxivarà 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.

1.4.1.3.3. Certificat d'Entitat d'Identificació, Xifrat i Signatura Electrònica Avançada de classe 1 (CEIXSA-1)

Els certificats d'entitat d'identificació, xifrat i signatura electrònica avançada de classe 1 són certificats reconeguts, no emesos al públic, d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emesos complint les obligacions dels articles 7, 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456 .

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

1.4.1.4. Certificats de dispositiu

1.4.1.4.1. Certificats de dispositiu de servidor segur de classe 1 (CDS-1)

Els certificats de dispositiu servidor segur (CDS) s'emeten a persones físiques o persones jurídiques, 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, amb caràcter general, certificats ordinaris que garanteixen la identitat de la persona jurídica responsable i dels servidors concrets on funcionen.

1.4.1.4.2. Certificats de dispositiu de servidor segur de classe 1 Extended Validation (CDS-1 EV)

Els CDS-1 EV s'emeten a les Institucions, 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
- Validació automàtica del certificat mitjançant els navegadors web adherits a CABForum.

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

1.4.1.4.3. Certificat de dispositiu de seu electrònica de classe 1 Extended Validation (CDS-1 Seu nivell mig i alt EV)

Els CDS--1 de seu electrònica Extended Validation s'emeten a les Universitats i Centres de Recerca, responsables de l'operació de servidors segurs SSL o TLS, amb la finalitat d'identificar i garantir una comunicació segura amb la seu electrònica d'un ens, entenent-se seu electrònica en els termes de l'article 10 de la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics. Es tracta de certificats reconeguts que poden utilitzar-se per a la connexió segura dels ciutadans a pàgines web oficials, l'autenticació d'un lloc web, l'allotjament de registres electrònics, la consulta i autorització de registres de representació, etc.

Es distingeixen dos certificats:

- El certificat de nivell mig, amb unes claus de 1024 bits, és recomanable per a la majoria de les administracions públiques amb previsió dels següents riscos: infracció de seguretat (per exemple, robatori de la identitat), pèrdues econòmiques moderades, pèrdua d'informació sensible o crítica, o refutació d'una transacció amb impacte econòmic significatiu.
- El certificat de nivell alt, emmagatzemat en un HSM (maquinari criptogràfic), i amb unes claus de 2048 bits, és recomanable per a aquelles administracions públiques que, havent realitzat prèviament una anàlisi de riscos, precisen mesures addicionals de seguretat, al contemplar els següents riscos: infracció de seguretat, pèrdues econòmiques importants,

pèrdua d'informació altament sensible i crítica o refutació d'una transacció amb impacte econòmic molt significatiu.

Aquests certificats incorporen la funció Extended Validation, que permet la validació automàtica del certificat mitjançant els navegadors adherits a CABForum.

1.4.1.4.4. Certificats de dispositiu segur de controlador de domini de classe 1 (CDSCD-1)

Els CDSCD s'emeten a les Universitats i Centres de Recerca de les Institucions 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.

1.4.1.4.5. Certificats de dispositiu d'Aplicació digitalment assegurada de classe 1 (CDA-1)

Els CDA s'emeten a les Universitats i Centres de Recerca responsables de l'operació d'aplicacions informàtiques que s'identifiquen digitalment, que signen electrònicament webservices o altres protocols i que reben documents i missatges xifrats.

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

1.4.1.4.6. Certificats de dispositiu d'aplicació digitalment assegurada segell electrònic de classe 1 (CDA-1 segell electrònic nivell mig i alt)

Els CDA-1 segell electrònic s'utilitzen per a la identificació i l'autenticació de l'exercici de la competència en l'actuació administrativa automatitzada, en els termes descrits en l'article 18 de la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics.

Aquest certificat pot utilitzar-se per a l'intercanvi de dades entre administracions, la identificació i autenticació d'un sistema, servei web o aplicació, l'arxiu electrònic automatitzat, les compulses i còpies electròniques, entre altres. Es distingeixen dos certificats:

- El certificat de nivell mig, lliurat en format software i amb unes claus de 1024 bits, és recomanable per a la majoria de les administracions públiques que poden tenir els següents riscos: infracció de seguretat (per exemple robatori de la identitat), pèrdues econòmiques moderades, pèrdua d'informació sensible o crítica, o refutació d'una transacció amb impacte econòmic significatiu.
- El certificat de nivell alt, carregat directament en la PSIS (Plataforma de serveis d'identificació i signatura), i amb unes claus de 2048 bits, és recomanable per a aquelles administracions públiques que, havent realitzat prèviament una anàlisi de riscos, precisen mesures addicionals de seguretat, ja que contempnen els següents riscos: infracció de seguretat, pèrdues econòmiques importants, pèrdua d'informació

altament sensible i crítica o refutació d'una transacció amb impacte econòmic molt significatiu.

1.4.1.4.7. Certificats de dispositiu de signatura de programari de classe 1 (CDP-1)

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 que garanteixen la identitat de la persona jurídica responsable i l'origen i la integritat del programari signatura.

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 a 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 severos.

1.4.2.2. Certificat d'infraestructura personal d'identificació i de signatura reconeguda

Qualsevol altre ús no especificat a la secció anterior està expressament prohibit i la seva detecció donarà lloc a la immediata revocació del certificat CIPISR.

1.4.2.3. Certificats personals d'identificació i signatura electrònica reconeguda

Els certificats CIPISR-1 amb Càrrec, CIPISR-1 amb Càrrec Estrangers, CIPISR-1 amb Càrrec ús, CIPISR-2 amb Càrrec, CIPISR-2 d'Estudiant i CIPISR-2 d'Estudiant Estranger, no es poden utilitzar per a:

- Signar peticions d'emissió, renovació, suspensió, habilitació 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.

1.4.2.4. Certificat personal d'identificació, xifrat i signatura avançada

Els certificats CPIXSA-1 Càrrec EP no es poden utilitzar 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).

1.4.2.5. Certificats personals de xifrat

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

1.4.2.6. Certificats d'entitat d'identificació i signatura electrònica reconeguda

Els certificats CEISR no es poden utilitzar per a:

- Signar peticions d'emissió, renovació, suspensió, habilitació 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.

1.4.2.7. Certificats d'entitat de xifrat

Els CEX no es poden utilitzar per generar signatures electròniques de cap tipus de missatge de dades.

1.4.2.8. Certificat d'entitat d'identificació, xifrat i signatura electrònica avançada

Els CEIXSA no es poden utilitzar per a:

- Signar peticions d'emissió, renovació, suspensió, habilitació o revocació de certificats.
- Signar certificats de clau pública de cap tipus, ni llistes de revocació de certificats (LRC).
- Realitzar signatura electrònica reconeguda de documents

1.4.2.9. Certificats de dispositiu de servidor segur

Els CDS-1 y els CDS-1 EV no es poden utilitzar per signar peticions d'emissió, renovació, suspensió, habilitació o revocació de certificats CIC, certificats de cap tipus o llistes de revocació de certificats (LRC).

1.4.2.10. Certificats de dispositiu de servidor segur de seu electrònica

Els CDS-1 de Seu electrònica EV no es poden utilitzar per a assegurar servidors que no tinguin la consideració legal de seu electrònica.

1.4.2.11. Certificats de dispositiu segur de controlador de domini (CDSCD)

Els CDSCD no es poden utilitzar per a signar peticions d'emissió, renovació, suspensió, habilitació o revocació de certificats CIC, certificats de cap tipus o llistes de revocació de certificats (LRC).

1.4.2.12. Certificats de dispositiu d'aplicació digitalment assegurada

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

Així mateix, no es poden utilitzar per assegurar aplicacions diferents a la identificada al certificat.

1.4.2.13. Certificats de dispositiu d'aplicació digitalment assegurada de segell electrònic

Els CDA de segell electrònic no es poden utilitzar per a la realització d'actes manuals.

1.4.2.14. Certificats de dispositiu de signatura de programari

Sense estipulació addicional.

1.5. Administració de la Declaració de Pràctiques de Certificació

1.5.1. Organització que administra l'especificació

Adreça postal:	
<u>Centre de Supercomputació de Catalunya (CESCA)</u> Gran Capità, 2-4 (Edifici Nexus) 08034 Barcelona	Agència Catalana de Certificació Passatge de la Concepció, 11 08008 Barcelona
Adreça web:	
http://www.cesca.es http://www.cesca.es/scd (informació sobre subscripcions)	http://www.catcert.cat
Telèfon:	
+34 93 205 64 64	+34 93 272 26 00

Correu-e:		
resp_scd@cesca.es (informació sobre subscripcions)		scd@catcert.cat
Fax:		
+34 93 205 69 79		+34 93 272 25 39

1.5.2.Dades de contacte de l'organització

Adreça postal:		
<u>Centre de Supercomputació de Catalunya (CESCA)</u> Gran Capità, 2-4 (Edifici Nexus) 08034 Barcelona		Agència Catalana de Certificació Passatge de la Concepció, 11 08008 Barcelona
Adreça web:		
http://www.cesca.es http://www.cesca.es/scd (informació sobre subscripcions)		http://www.catcert.cat
Telèfon:		
+34 93 205 64 64		+34 93 272 26 00
Correu-e:		
resp_scd@cesca.es (informació sobre subscripcions)		scd@catcert.cat
Fax:		
+34 93 205 69 79		+34 93 272 25 39

1.5.3. Persona que determina la conformitat d'una DPC amb la política

Adreça postal:	
<u>Centre de Supercomputació de Catalunya (CESCA)</u> Gran Capità, 2-4 (Edifici Nexus) 08034 Barcelona	Agència Catalana de Certificació Passatge de la Concepció, 11 08008 Barcelona
Adreça web:	
http://www.cesca.es http://www.cesca.es/scd (informació sobre subscripcions)	http://www.catcert.cat
Telèfon:	
+34 93 205 64 64	+34 93 272 26 00
Correu-e:	
resp_scd@cesca.es (informació sobre subscripcions)	scd@catcert.cat
Fax:	
+34 93 205 69 79	+34 93 272 25 39

1.5.4. Procediment d'aprovació

El procediment per l'aprovació i modificació d'aquesta declaració de pràctiques serà l'establert al Conveni marc de col·laboració entre el Departament d'Universitats, Recerca i Societat de la Informació, la Fundació Catalana per a la Recerca, la Universitat de Barcelona, la Universitat Autònoma de Barcelona, la Universitat Politècnica de Catalunya, la Universitat Pompeu Fabra, la Universitat de Girona, la Universitat de Lleida, la Universitat Rovira i Virgili, la Universitat Oberta de Catalunya, l'Associació Catalana d'Entitats de Recerca, Serveis Públics Electrònics (CAT365), l'Agència Catalana de Certificació i el Consorci Centre de Supercomputació de Catalunya, de 23 d'octubre de 2003, que preveu la seva aprovació definitiva per la Comissió Mixta de Seguiment i Control del Conveni Marc a la seva clàusula desena.

2. Publicació d'informació i directori de certificats

2.1. Directori de certificats

El Directori 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-UR, 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-UR

L'EC-UR publica les següents informacions, en el seu web (<http://www.catcert.cat/>):

- a) Les llistes de certificats revocats i altres informacions d'estat de revocació dels certificats.
- b) La política general de certificació
- c) Els perfils dels certificats i de les llistes de revocació dels certificats.
- d) La Declaració de Pràctiques de Certificació.
- e) 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-UR.

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-UR 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 directori.

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

2.4. Control d'accés

L'EC-UR 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-UR utilitza sistemes fiables per al Directori, de tal manera que:

- Es pugui comprovar l'autenticitat dels certificats.
- Les persones no autoritzades no puguin alterar les dades.
- 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

3.1.1.1. Estructura sintàctica

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

L'estructura sintàctica i el contingut dels camps de cada certificat, així com el seu significat semàntic es troba descrit al document "perfil de certificat" corresponent, que l'Agència Catalana de Certificació publica en el seu web (<http://www.catcert.cat/>).

3.1.1.2. Perfils dels certificats

Els perfils dels certificats emesos per l'EC-UR es publiquen als webs de CATCert i del CESCA (<http://www.catcert.cat/> i <http://www.cesca.cat/>).

3.1.1.3. Característiques dels certificats personals de classe 1 amb càrrec

El llistat de categories per al camp Title 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 de recerca
- "PAS" Personal d'Administració i Serveis
- "PDI" Personal Docent i Investigador
- "PVE" Personal Vinculat o Extern

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

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

- "EST " Estudiants.
- "EST EST" Estudiants estrangers

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-UR emet diferents tipus de certificats. Una mateixa persona (o un mateix posseïdor de claus) pot disposar de diversos certificats del mateix tipus en diverses institucions que integren la EC-UR, així com diversos tipus de certificat dins de la mateixa Institució.

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 o els posseïdors de claus 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-UR no determina que un sol·licitant o un posseïdor de claus 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-UR 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, de:

- 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 que són part de l'Acord Schengen i que no tenen el NIE, el document nacional d'identitat del país d'origen o de procedència o passaport vigent del posseïdor de claus.
- V.gr.: italià (C) = IT; (SN) = IT-Document nacional d'identitat
- En cas d'estrangers nacionals d'Estats que no són part de l'Acord Schengen i que no tenen el NIE, el Passaport ordinari, diplomàtic, oficial o de servei, del posseïdor de claus vàlidament expedit i en vigor.
- V.gr.: xinès (C) = CN; (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 per el subscriptor.
- V.gr.: un número de carnet de la Universitat o Institució corresponent.

Aquest sistema de resolució de conflictes de noms respon al fet que les organitzacions subscriptores dels certificats identificades com a tals en el camp "Organizational Unit Name" del "Subject" del perfil dels certificats, estan sotmeses al Dret espanyol.

La submissió al Dret espanyol ve determinada per la RFC 3739, que estableix que el camp "Subject" contindrà, entre altres atributs, l'atribut "countryName" el valor del qual consisteix a especificar el context en el qual s'han d'entendre definits els altres atributs del "Subject", és a dir, sobre la base de la normativa de quin país hem d'entendre semànticament els altres camps del "Subject". És llavors, amb base en el "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 norma general, entorn a la seva nacionalitat. Per tant, per a 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 d'Identitat d'Estrangers.

Aquells estrangers que no tinguin el NIE s'identificaran amb la corresponent documentació acreditativa, que variarà en funció de la nacionalitat de l'estranger, diferenciant-se entre els nacionals d'Estats part en l'Acord Schengen i els altres. Els primers acreditaran la seva identitat mitjançant la presentació del seu document nacional d'identitat o del seu passaport vàlidament expedit i en vigor. I els segons, ho acreditaran mitjançant el passaport, el títol de viatge o el document nacional d'identitat, cèdula d'identificació o qualsevol altre document que acrediti la seva identitat en virtut de compromisos internacionals, en els quals quedi perfectament reflectida 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 en els 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.

En cas que el nom a incloure en el certificat sigui excessivament llarg, es procedirà a abreviar algun dels noms i mai el primer cognom.

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, qualsevol 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 parell de claus emmagatzemades en el seu interior.

Quan el parell de claus és generat per l'Entitat de Registre, no és el sol·licitant qui ha de demostrar la possessió de la clau privada, sinó l'Entitat de Registre, que ho fa en virtut del procediment fiable d'emissió, de lliurament i d'acceptació del dispositiu segur i del corresponent certificat i parell de claus emmagatzemats al seu interior.

Ha d'assegurar-se que únicament el posseïdor de claus de certificats d'organització té únicament la clau de signatura.

3.2.2. Autenticació de la identitat d'una Organització

Aquesta secció conté els requisits per a la comprovació de la identitat d'una organització identificada en el certificat.

3.2.2.1. Entitats de Registre

L'EC-UR autenticarà, amb caràcter previ a l'emissió i entrega d'un certificat d'operador, per a qualsevol dels components d'una Entitat de Registre, la identitat de l'Entitat de Registre i de l'operador.

Per a tal fi, l'EC-UR utilitzarà algun dels següents mètodes:

- 1) Obtenció d'informació sobre l'organització, d'un proveïdor extern de serveis d'aquesta naturalesa
- 2) Comprovació de la documentació justificativa aportada pel sol·licitant. En aquest cas, es requerirà la presència física del representant de la futura Entitat de Registre.

3.2.2.2. Subscriptors de certificats

3.2.2.2.1. Requisits per a certificats de classe 1

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

3.2.2.2.2. Requisits per a certificats de classe 2

És necessari autenticar, amb caràcter previ a l'emissió i entrega del certificat, la identitat del subscriptor i d'altres dades establertes a la secció corresponent per a aquest tipus de certificats.

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) Nombre d'identificació fiscal
- d) Dades d'identificació registral

3.2.2.2.3. Requisits específics per als certificats de dispositiu servidor segur i els certificats de controlador de domini

Sense perjudici de les mesures establertes a les Condicions Generals d'Ús, en el cas dels certificats de dispositiu de servidor segur (inclosos els de seu electrònica) i certificats de controlador de domini, i addicionalment a la comprovació que s'hagi de dur a terme de l'organització responsable del servidor segur, es comprova:

- L'existència del servidor.
- La titularitat del nom de domini provinent del registre corresponent.
- L'autorització per a l'organització de l'emissió del certificat en el servidor.

3.2.2.2.4. Requisits específics per al CDA

En el cas dels certificats de dispositiu d'aplicació digitalment assegurada, addicionalment a la comprovació que s'hagi de dur a terme de l'organització responsable de l'aplicació informàtica, es comprova:

- L'existència i la titularitat de l'aplicació informàtica.
- L'autorització per a l'organització de l'emissió del certificat en el dispositiu corresponent.

3.2.2.2.5. Requisits específics per al CDP

En el cas dels certificats de dispositiu de signatura de software, addicionalment a la comprovació que s'hagi de dur a terme de l'organització responsable del software, es comprova:

- L'existència i la titularitat del software.
- L'autorització de l'organització per a l'emissió del certificat en el dispositiu corresponent.

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 requerits

El nombre i tipus de documents necessaris per a acreditar la identitat del posseïdor de claus són els que admet cada organització subscriptora 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
- Número d'identitat reconegut legalment (DNI, NIF o NIE dels països signataris de l'Acord Schengen; passaport en el cas dels certificats d'estranger).
- Qualsevol altra informació que pugui ser utilitzada per diferenciar una persona de l'altra, dins de l'àmbit de la Institució (per exemple: fotografia, correu-e, categoria, càrrec, etc.).

3.2.3.2. Validació dels elements d'identificació

La informació d'identificació de posseïdors de claus de certificats de Classe 1 es valida comparant la informació de la sol·licitud amb els registres interns de l'Entitat de Registre que s'assegura de la correcció de la informació a certificar.

La informació d'identificació de posseïdors de claus de certificats de Classe 2 es valida comparant la informació de la sol·licitud amb la informació dels estudiants de nou ingrés que prové dels llistats tramitats per la Generalitat, d'acord amb la normativa de pre-ingrés universitari.

Es pot ocupar un proveïdor corporatiu d'informació de recursos humans per a aquesta tasca.

La informació del posseïdor registrada per la Universitat o Centre 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 Institució, i que ho fa mitjançant la seva relació funcional, 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 Institució

Com que es tracta de certificats corporatius, en què 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 no verificada

La Universitat o Centre es responsabilitza que tota la informació inclosa a la sol·licitud del certificat sigui exacta i 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. Si més no, si la renovació es realitza durant els 5 primers anys des de la primera comprovació de la identitat, dita identificació no serà necessària.

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

La renovació de certificats després de la revocació no és possible.

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

Nota: el terme “notificació” s'utilitza en aquest document com a equivalent de “comunicació”, excepció feta de les tramitacions documentals amb d'altres organismes públics exigibles per la legislació aplicable.

4.1. Sol·licitud d'emissió de certificat

4.1.1. Legitimació per a sol·licitar certificats

4.1.1.1. Certificats personals, d'entitat i de xifrat.

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 documentació acreditativa es genera mitjançant tres processos alternatius:

1. L'acte administratiu de certificació prèvia de les dades, per part de la institució sol·licitant del certificat, enfront del CESCA, que és l'Entitat de Registre de l'Entitat de Certificació.

L'EC-UR informa al subscriptor dels termes i condicions aplicables al certificat, en llenguatge fàcilment comprensible.

La sol·licitud és, en qualsevol cas, el primer pas que ha de fer el subscriptor per aconseguir els certificats per al seu personal. Una Addenda al Conveni signat entre CATCert i el CESCA determinarà la persona o persones autoritzades per sol·licitar certificats a l'EC-UR en nom del subscriptor. Aquesta sol·licitud requereix la tramesa d'un document amb la informació exacta i comprovada (certificada) de les persones o dispositius per a les que es demana el certificat. Aquesta sol·licitud se signa per part de la persona autoritzada pel subscriptor a la fitxa. També s'envia un certificat de dades. També es pot acompanyar d'una adreça física, o altres dades, que permetin establir contacte directe amb el futur posseïdor de claus.

Tota la documentació es lliura al Responsable del servei de certificació digital del CESCA presencialment, en suport paper, mitjançant correu postal certificat, o en suport electrònic, mitjançant correu electrònic signat i xifrat, o també telemàticament, sempre que escaigui per raons tècniques o d'aplicatiu informàtic.

2. L'acte administratiu de registre directe per una institució constituïda com a Entitat de Registre de l'Entitat de Certificació, d'acord amb el conveni corresponent signat per CATCert, CESCA i la Institució.

Per a que existeixi una sol·licitud primer disposem d'una relació entre la Institució i els posseïdors de claus. Aquesta relació pot definir-se de tres formes:

- Si són professors, a partir de la relació contractual entre la Institució i ells, ja siguin funcionaris o disposin d'un contracte laboral.
- Si són membres del PAS, a partir de la relació contractual entre la Institució i ells, ja siguin funcionaris o disposin d'un contracte laboral.
- Si són estudiants, a partir de la matrícula oficial a un programa reglat o a assignatures individuals.

Quan es demana un certificat CPISR-1 amb càrrec per a professors o membres del PAS, un membre de l'òrgan competent de la Institució fa la sol·licitud on consta la relació autenticada (per exemple, mitjançant un certificat administratiu) d'aquells usuaris que han de rebre un certificat, o s'obtenen les dades de manera automàtica dels sistemes de gestió d'identitat de la Institució. Aquest document es fa arribar a un responsable de l'Entitat de Registre, que segueix endavant amb el procés.

Quan es demana un certificat CPISR-2 d'estudiant, un membre de l'òrgan competent de la Institució fa la sol·licitud on consta la relació autenticada (per exemple, mitjançant còpia autèntica de la llista dels estudiants matriculats) d'aquells usuaris que han de rebre un certificat, o s'obtenen les dades de manera automàtica dels sistemes de gestió d'identitat de la Institució. Aquest document es fa arribar a un responsable de l'Entitat de Registre, que segueix endavant amb el procés.

- a) L'acte administratiu de registre directe per una institució constituïda, d'acord amb el conveni de referència, com Entitat de Certificació Vinculada a l'Entitat de Certificació, mitjançant la seva pròpia Entitat de Registre.
- b) Presència davant notari, d'acord amb l'article 13.1 de la Llei de Signatura Electrònica

4.1.1.2. 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, encarregat de l'Entitat de Registre. Aquesta sol·licitud només pot ser realitzada pels responsables de les unitats o departaments corresponents.

De la mateixa manera que pels certificats personal i d'entitat, l'encarregat de l'ens subscriptor ha de realitzar la tramitació telemàticament, quan escaigui.

4.1.2. Procediment d'alta; Responsabilitats de l'ER

En el cas que l'Entitat de Registre tingui connexió automàtica amb els sistemes de gestió d'identitat de la Institució, diàriament es genera un procés automàtic que revisa les bases de dades, corresponents a alumnes i a personal de les universitats que formen part del Conveni de referència, 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 UR.

La comunicació realitzada a l'AC de la UR 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 corresponent, que analitza i canalitza la resolució de les sol·licituds que han estat rebutjades.

L'Entitat de Certificació ha d'assegurar-se que les sol·licituds de certificat són completes, precises i estan degudament autoritzades.

Abans de l'emissió i lliurament del certificat, l'Entitat de Certificació informará el subscriptor, dels termes i condicions aplicables al certificat.

En certificats d'organització, aquest requisit es podrà complir lliurant l'instrument jurídic que vincula a l'Entitat de Certificació amb el subscriptor i lliurant un full de lliurament al posseïdor de claus, que inclogui aquesta informació.

L'esmentada informació es comunicarà en suport perdurable, en paper o electrònicament i en llenguatge fàcilment comprensible.

A la sol·licitud es podrà acompanyar documentació justificativa de la identitat del subscriptor i altres circumstàncies, i del posseïdor de claus, d'acord amb l'establert a la secció corresponent d'aquesta declaració de pràctiques de certificació.

També es podrà acompanyar una adreça física, o altres dades, que permetin contactar amb el subscriptor.

L'Entitat de Registre és la responsable de realitzar el procediment d'alta, que pot ser de dues maneres:

1. Procediment d'alta quan l'efectua el CESCA com a Entitat de Registre:

Una vegada el CESCA ha rebut l'addenda al conveni de col·laboració amb la fitxa, signat pel subscriptor, s'obre l'expedient, incloent ambdós documents.

El CESCA dona d'alta en una base de dades la informació continguda a la fitxa de subscriptor inclosa al conveni, a fi de poder realitzar consultes posteriors, principalment sobre quines són les persones autoritzades per actuar en nom d'aquest subscriptor.

El CESCA lliura al subscriptor la documentació (model de formulari) necessària a fi de sol·licitar certificats o bé li indica la secció del web on la pot obtenir.

2. Procediment d'alta quan l'efectua l'Entitat de Registre:

Un membre de l'òrgan competent del subscriptor fa la corresponent sol·licitud on hi consta la relació autenticada dels usuaris que han de rebre un certificat, fent-la arribar a un responsable de l'Entitat de Registre qui segueix endavant amb el procés, o s'obtenen les dades de manera automàtica dels sistemes de gestió d'identitat de la Institució.

4.2. Processament de la sol·licitud de certificació

4.2.1. Certificats personals

4.2.1.1. Quan el CESCA actua com a Entitat de Registre:

Quan el CESCA rep una nova sol·licitud de certificat, en primer lloc registra la documentació, que s'afegeix a l'expedient del subscriptor.

El CESCA s'assegura que les sol·licituds de certificats són completes, precises i estan degudament autoritzades i arxivades.

Si falta algun document, el CESCA ho comunica al subscriptor per correu electrònic signat, perquè l'aporti, ja que el procés de sol·licitud de certificats queda aturat fins que no es disposi de tota la documentació.

Posteriorment, una persona autoritzada pel CESCA accedeix al sistema de certificació i un cop identificada, introdueix totes les dades que el sistema li demana, obtenint-los de

l'expedient anteriorment indicat i que conté la documentació necessària (ja sigui en paper o en format electrònic).

Una vegada introduïdes totes les dades, aquestes es verifiquen d'acord amb la informació de la sol·licitud i la documentació de l'expedient.

Si la sol·licitud és correcta, el CESCA:

- Aprova la sol·licitud.
- Genera el parell de claus.
- Sol·licita a l'EC-UR la generació del certificat.

Si la sol·licitud presenta incorreccions que no es poden corregir, el CESCA la denega definitivament.

4.2.1.2. Quan s'efectua el processament per una Entitat de Registre:

L'Entitat de Registre rep una nova sol·licitud de certificat provinent de l'òrgan competent de la Institució (per exemple del Departament de Recursos Humans, del Rectorat, del Gerent, del Departament de Matriculació, de la Secretaria Docent, etc).

El procediment segueix mitjançant expedients en paper, correu electrònic o tramitació telemàtica, amb la signatura electrònica reconeguda basada en un certificat CPISR-1 amb càrrec emès per l'EC-UR.

L'usuari (professor, membre del PAS o estudiant) es persona físicament a l'Entitat de Registre, amb la seva targeta.

Un cop identificat amb l'original del DNI, NIE o equivalent insereix la targeta en la unitat de gravació.

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

- Aprova la sol·licitud.
- Genera el parell de claus, dins de la targeta del futur posseïdor de claus.
- Sol·licita a l'EC-UR la generació del certificat.

4.2.2. Requisits específics per al CEIXSA

Una vegada aprovada la sol·licitud, la EC-UR rep l'autorització de l'Entitat de Registre, recupera la corresponent sol·licitud de la taula de sol·licituds, l'emmagatzema en l'estructura de certificats, sent signada per la EC-UR, completant així la generació del certificat.

A partir d'aquest moment el sol·licitant ja pot descarregar des de la web el seu certificat i començar a utilitzar-lo.

4.2.3. Informacions addicionals per al CDS, el CDS-1 EV, el CDSCD i el CDS-1 Seu electrònica EV

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-UR procedeix a l'emissió del certificat.

Els certificats digitals de dispositiu es lliuraran mitjançant un fitxer que haurà de descarregar-se el responsable de l'Entitat de Registre.

4.2.4. Requisits específics per al CIPISR

Addicionalment, l'Entitat de Certificació haurà de:

- Incloure al certificat les informacions establertes a l'art. 11 de la Llei 59/2003, d'acord amb l'establert a la secció 7 d'aquesta política.
- Garantir la data i l'hora en què es va expedir un certificat
- En cas que l'Entitat de Certificació porti el dispositiu segur de creació de signatura, emprar un procediment de gestió de dispositius segurs de creació de signatura que asseguri que l'esmentat dispositiu és lliurat de forma segura al posseïdor de claus.
- Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, en el seu cas, criptogràfica dels processos de certificació als que serveixen de suport.
- Assegurar-se que el certificat és emès per sistemes que utilitzin protecció contra falsificació i, en cas que l'Entitat de Certificació generi claus privades, que garanteixin el secret de les claus durant el procés de generació de les esmentades claus

4.2.5. Altres certificats

Les sol·licituds realitzades són processades i es realitza la validació. En el cas que tot sigui correcte, es crea la sol·licitud en l'EC-UR. 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.

4.3. Emissió de certificat

4.3.1. Accions de l'EC-UR 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-UR ha de:

- Utilitzar un procediment de generació de certificats que vinculi de forma segura el certificat amb la informació de registre, incloent-hi la clau pública certificada

- En cas que l'Entitat de Certificació generi el parell de claus, utilitzar un procediment de generació de certificats vinculat de forma segura amb el procediment de generació de claus i, que la clau privada és lliurada de forma segura al subscriptor, en cas de certificats individuals, o al posseïdor de claus en cas de certificats d'organització.
- Protegir la confidencialitat i integritat de les dades de registre, especialment en cas de que siguin intercanviats amb el subscriptor, en cas de certificats individuals, amb el posseïdor de claus, en cas de certificats d'organització o amb el tercer sol·licitant, en el seu cas.
- Incloure en el certificat les informacions establertes en l'art. 11.2 de la Llei 59/2003, d'acord amb allò establert la secció corresponent d'aquesta política.
- Indicar la data i l'hora en les que es va expedir un certificat.
- En cas de que l'Entitat de Certificació porti el dispositiu segur de creació de signatura, utilitzar un procediment de gestió de dispositius segurs de creació de signatura que assegurí que aquest dispositiu és lliurat de forma segura al posseïdor de claus.
- Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, en el seu cas, criptogràfica dels processos de certificació als que serveixen de suport.
- Prendre mesures contra la falsificació de certificats i, en cas que l'Entitat de Certificació generi claus privades, que garanteixin el secret de les claus durant el procés de generació d'aquestes claus.

4.3.2. Notificació de l'emissió al subscriptor

L'EC-UR notifica al subscriptor l'emissió del certificat o la incidència corresponent.

4.4. Acceptació del certificat

4.4.1. Responsabilitats de l'Entitat de Registre en el procediment d'alta

4.4.1.1. Per a Certificats personals

El CESCA és l'encarregat de crear el parell de claus i el certificat dels subscriptors.

El CESCA també crea els corresponents codis PIN i PUK de les targetes (dispositius criptogràfics) on s'allotgen el parell de claus i el certificat. Per a cada posseïdor genera dues còpies del full de lliurament; una per al posseïdor i l'altra per al subscriptor.

Aquests codis es podran reenviar directament al posseïdor de claus, que els podrà sol·licitar a través de l'aplicació telemàtica en qualsevol moment.

Al full de lliurament de subscriptor s'indica a aquest:

- que s'ha demanat prèviament al responsable del servei de l'Entitat de Registre documentació completa i adequada de les dades dels respectius posseïdors, per a la seva identificació i relació amb el subscriptor,

- que aquest responsable del servei de l'Entitat de Registre es compromet a lliurar les targetes i els certificats als posseïdors, informar-los de les seves obligacions i responsabilitats, i a custodiar el full de lliurament de posseïdor degudament signat durant 15 anys,
- es demana al posseïdor que estigui informat sobre el tractament de les seves dades, respecte de la normativa de protecció de dades i que doni consentiment per al tractament i la inclusió de certes dades al certificat.

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

Els certificats de dispositiu es lliuraran mitjançant un fitxer que haurà de descarregar-se el responsable de l'entitat de registre virtual.

L'EC-UR generarà el full de lliurament per a cada posseïdor de claus. CATCert enviarà mitjançant correu electrònic directament als posseïdors de claus els codis PIN i PUK, si escau, segons el tipus de certificat.

Aquests codis es podran reenviar directament pel posseïdor de claus, que els podrà sol·licitar a través de l'aplicació telemàtica en qualsevol moment.

4.4.2. Conducta que constitueix acceptació del certificat

El certificat s'accepta mitjançant la signatura del full de posseïdor de claus.

També es pot acceptar mitjançant un mecanisme telemàtic d'activació del certificat.

A través de l'aplicació telemàtica es podran obtenir informes de tots els certificats gestionats per l'Entitat de Registre Virtual en el moment actual o un recull històric.

4.4.2.1. Informacions addicionals per al CEIXSA

El subscriptor accepta el certificat, descarregant-lo de la web i no retornant-lo en 7 dies.

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 del parell de claus pels posseïdors de claus i ús del certificat pels subscriptors

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 les Institucions, entre elles, 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 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.

S'ha de tenir en compte que es dona 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 les Entitats de Certificació.

4.5.1.2. Informacions addicionals per als certificats personals

Els certificats personals i de dispositiu no es poden utilitzar per signar altres certificats, o informació d'estat de certificats, de cap manera.

4.5.1.3. Informacions addicionals per al CIPISR

Els CIPISR 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 CPISR

Els CPISR 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.

4.5.1.5. Informacions addicionals per al CPX

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

4.5.1.6. Informacions addicionals per al CEISR

Els CEISR s'utilitzen necessàriament amb un dispositiu segur de creació de signatura electrònica, que compleix les característiques establertes per l'article 24.3 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.

4.5.1.7. Informacions addicionals per al CEX

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

4.5.1.8. Informacions addicionals per al CEIXSA

S'és especialment diligent en la custòdia de la clau privada amb la finalitat d'evitar usos no autoritzats.

4.5.1.9. Informacions addicionals per als CDS-1 y els CDS-1 EV

Els CDS-1 i els CDS-1 EV han d'utilitzar-se en conjunció amb un dispositiu de protecció de la clau privada de desxifrat, de conformitat amb els requisits establerts en la política de certificació i les Condicions Generals d'Ús.

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 dona 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-UR.

4.6. Renovació de certificats sense renovació de claus

No es permet la renovació de certificats sense renovació de claus.

4.7. Renovació de certificats amb renovació de claus

La renovació d'un certificat s'inicia dos mesos abans de la data d'expiració del certificat, quan el subscriptor rep un correu electrònic on se l'informa dels passos a seguir per a executar la renovació del certificat. Aquest correu electrònic es torna a enviar 30 dies abans de l'expiració.

El procés per la renovació d'un certificat és el mateix que es segueix per a l'emissió de nous certificats. En qualsevol cas, si han passat més de cinc anys des de la darrera vegada que el subscriptor es va identificar presencialment a una oficina d'entitat de registre, cal presentar-se de nou per a dur a terme la renovació.

4.8. Modificació de certificats

El sol·licitant d'un certificat haurà de requerir la modificació dels certificats quan tingui coneixement de canvis en la informació obligatòria o la relativa a càrrecs, límits d'ús o dispositius usuaris dels certificats (p.ex. adreces IP o dades de servidors o aplicacions). Així mateix, podrà requerir la modificació de la resta de dades incloses al certificat. Per tal de realitzar les modificacions, l'Entitat de Registre podrà requerir l'acreditació de les condicions justificatives de la modificació. La modificació de les dades dels certificats comporta la revocació i l'emissió d'un nou certificat. A tots els efectes, la modificació es considerarà renovació.

4.9. Revocació i suspensió de certificats

4.9.1. Causes de revocació de certificats

L'EC-UR pot revocar un certificat per alguna de 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 incorrecta.
2. Circumstàncies que afecten a la seguretat de la clau o del certificat
 - Compromís de la clau privada o de la infraestructura o sistemes de l'EC-UR, sempre que afecti la confiança en els certificats emesos a partir d'aquest incident.
 - Infracció, per part de l'EC-UR, 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 autoritzada, per part d'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 la seguretat del dispositiu criptogràfic
 - Compromís o sospita de compromís de la seguretat del dispositiu criptogràfic.
 - Pèrdua o inutilització per danys del dispositiu criptogràfic.
 - Accés no autoritzat, per part d'un tercer, a les dades d'activació del subscriptor.
4. Circumstàncies que afecten el subscriptor o el posseïdor de claus
 - Final de la relació entre l'EC-UR i el subscriptor.
 - Modificació o extinció de la relació jurídica subjacent o causa que va provocar l'emissió del certificat al subscriptor.
 - Infracció per part del sol·licitant del certificat dels requisits preestablerts per a la sol·licitud d'aquest.
 - Infracció per part del subscriptor de les seves obligacions, responsabilitats i garanties, establertes a l'instrument jurídic corresponent de l'EC-UR.
 - 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.
5. Circumstàncies relatives als certificats Extended Validation

- Sol·licitud del subscriptor.
- L'Entitat de Certificació obté proves raonables de que la clau privada del subscriptor s'ha vist compromesa o que el certificat ha estat usurpat per un tercer.
- L'Entitat de Certificació rep notificació o comunicació per part d'un tribunal o àrbitre sobre la revocació del dret a utilitzar el nom de domini que figura en el certificat, o coneix la impossibilitat de renovar el domini.
- L'Entitat de Certificació té coneixement de l'incompliment de les Condicions Generals d'Ús o d'altres especificacions establertes a la documentació jurídica o operativa.
- L'Entitat de Certificació cessa activitats que donin suport a la revocació de certificats Extended Validation o perd el dret d'emetre certificats Extended Validation. Si l'Entitat de Certificació pot garantir el manteniment dels serveis de validació CRL i OCSP, la revocació no és necessària.
- Compromís o sospita de compromís de les claus de qualsevol Entitat de Certificació de nivell superior en la jerarquia.
- Revocació de les publicacions de les polítiques relatives a certificats Extended Validation.
- Notificació de la inclusió d'un subscriptor al llistat de subscriptors prohibits (altrament, llistes negres, confeccionades per a víctimes de phishing o activitats d'enginyeria inversa).

6. Altres circumstàncies

- La suspensió del certificat digital per un període superior a 120 dies.
- El final del servei de l'EC-UR, d'acord amb l'establert a la secció 5.8 d'aquest document.
- La finalització de prestació de serveis per part de CATCert, d'acord amb el que estableix la Política General de Certificació.
- Resolució judicial o administrativa que ho ordeni (Art. 8.1 de la Llei 59/2003, de signatura electrònica).
- L'EC-UR té coneixement que els CDP han realitzat signatures sobre codi hostil.

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 (habilitació) i el certificat torna a passar a la situació de vàlid.

L'instrument jurídic que vincula l'EC-UR amb el subscriptor estableix que el subscriptor 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

La sol·licitud de revocació pot ser demanada pel subscriptor del certificat, CATCert, el CESCA o l'Entitat de Registre que va sol·licitar l'emissió del certificat. Els posseïdors de claus hauran de comunicar al subscriptor les circumstàncies previstes per la llei o aquesta Declaració i que poden donar lloc a la revocació del certificat que, en el seu cas, haurà de ser sol·licitada pel subscriptor.

4.9.3. Procediment de sol·licitud de revocació

El procediment de revocació es duu a terme per un dels operadors de l'Entitat de Registre, 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.

La sol·licitud de revocació ha de ser lliurada presencialment, enviada per correu electrònic signat o per correu certificat convencional. S'ha d'incloure la informació suficient per poder identificar raonablement, a criteri de l'EC-UR, d'una banda, el certificat que se sol·licita revocar i, d'altra banda, l'autenticitat i autoritat del sol·licitant.

Aquesta informació suficient ha d'estar composta per les dades de contacte del posseïdor de claus inclòs el seu DNI o equivalent, i de l'entitat que demana la revocació, la data i la raó de la petició, així com el número de sèrie del certificat.

Qui faci la sol·licitud de revocació pot demanar a l'Entitat de Registre més informació sobre aquest procediment.

La petició de revocació amb la documentació necessària és recollida i registrada per l'Entitat de Registre, que realitzarà la revocació en l'aplicació telemàtica i, a continuació i de forma automàtica i quasi immediata, s'inclourà l'esmentada revocació a la llista de certificats revocats. S'informa el subscriptor i, en el seu cas, el posseïdor de claus, sobre el canvi d'estat de revocació del certificat d'acord amb l'art. 10.2 de la Llei de signatura electrònica.

L'EC-UR 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.

4.9.6. Obligació de consulta d'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-UR. L'estat de vigència també es pot comprovar online mitjançant el protocol OCSP.

L'EC-UR 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-UR emet una LRC almenys cada 24 hores. A més s'emet una nova LRC després de cada suspensió o revocació.

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, cada cop que es revoqui o suspengui un certificat.

Els certificats revocats o suspesos 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 web de CATCert (<http://www.catcert.cat/>).

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 la LRC per comprovar la validesa d'un certificat, ho pot fer en el directori de l'EC-UR.

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-UR.

L'EC-UR 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-UR també informará sobre la revocació dels certificats, mitjançant el protocol OCSP, que permet conèixer l'estat de vigència dels certificats on-line.

En la petició de consulta de vigència d'un certificat en línia s'ha de consignar un numero de sèrie del certificat sobre el qual es fa la petició i les dades identificatives de l'autoritat de certificació emissora.

Si la petició no està vàlidament realitzada o si el servei no pot donar una resposta en el moment de la sol·licitud, el servei OCSP retornará una resposta que identifiqui el motiu pel qual no es torna aquesta resposta (sol·licitant no autoritzat, error en la resposta o inoperabilitat temporal del prestador requerit).

Si la petició està vàlidament realitzada i els serveis no tenen cap disfunció, es respondrà a la petició amb la consignació que el certificat és vàlid o que està revocat (en aquest cas es consignarà també el moment de la finalització de la vigència del certificat).

Aquesta resposta serà signada per l'Entitat de Certificació amb el certificat corresponent (en aquest cas, el certificat d'infraestructura de servidor d'estat de certificats en línia –que rep l'acrònim CIO). Aquesta resposta serà emmagatzemada.

4.9.12. Requisits especials en cas de compromís de la clau privada

El compromís de la clau privada de l'EC-UR és notificat, en la mesura del possible, a tots els participants en la jerarquia pública de certificació de Catalunya i a tots els tercers verificadors, mitjançant el dipòsit 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 o un tercer autoritzat (art. 9.1.a de la Llei 59/2003)
- En els casos legals previstos a l'article 9.1 de la Llei de Signatura Electrònica, és a dir, en cas que una resolució judicial o administrativa ho ordeni.
- Quan així sigui sol·licitat pel subscriptor o posseïdor de claus.
- 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 segon cas, l'EC-UR 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. Legitimitat per sol·licitar la suspensió

1. El posseïdor de claus del certificat
2. El subscriptor que va demanar l'emissió de certificats (Sol·licitant de l'Entitat de Registre).
3. Les Entitats de Certificació, que van emetre el certificat o altres Entitats de Registre.
- 4.

4.9.15. Procediments de sol·licitud de suspensió

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

La suspensió dels certificat digitals es pot realitzar de les formes que es detallen a continuació, tot informant al subscriptor d'acord amb els termes establerts a l'article 10.2 de la Llei de Signatura Electrònica:

1. La suspensió pot ser sol·licitada pel posseïdor de les claus i es pot dur a terme per via telefònica al 902 90 10 80.
2. La suspensió pot ser sol·licitada pel subscriptor del certificat i es pot realitzar per via telefònica al 902 90 10 80.
3. La suspensió pot ser sol·licitada pel CESCA o per l'Entitat de Registre. En cas que l'Entitat de Registre disposi d'autorització de CATCert, pot realitzar ella mateixa el procés de suspensió. En cas contrari, realitza la tramitació de la suspensió a través de CATCert.
4. La suspensió pot ser realitzada per l'EC-UR directament, a través del component LRA o RRA.

El procediment de suspensió es tramita de la mateixa manera que el procediment de revocació.

Per iniciar la suspensió es requereix la següent informació:

- Data i hora de la sol·licitud de la suspensió.
- Identitat del subscriptor que sol·licita la suspensió (en cas que no sigui el mateix posseïdor).
- Informació de contacte de l'entitat que demana la suspensió.
- Nom i cognoms del posseïdor de claus a qui se li ha de suspendre el certificat digital.
- DNI del posseïdor de claus a qui se li ha de suspendre el certificat digital.
- Organisme i departament a què pertany el posseïdor de claus.
- Número de sèrie (serial number) del certificat digital que se sol·licita suspendre.

- Raó detallada per a la petició de suspensió.
- Codi de suspensió associat al certificat..

Un cop suspesa la vigència d'un certificat s'informarà al subscriptor i, en el seu cas, al posseïdor de claus, sobre el canvi d'estat de suspensió i que el termini màxim de la mateixa serà de 120 dies (arts. 10.2 i 10.4 de la llei 59/2003).

4.9.16. Període màxim de suspensió

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

4.9.17. Habilitació d'un certificat suspès

El subscriptor podrà habilitar el certificat que roman suspès, personant-se i identificant-se davant l'Entitat de Registre, signant el corresponent document de sol·licitud d'habilitació, comunicant que s'ha extingit el motiu que va provocar la suspensió.

4.10. Serveis de comprovació d'estat de certificats

4.10.1. Característiques d'operació dels serveis

Les LRC són descarregades manualment des del directori de certificació de CATCert instal·lades pels 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 de fallida dels sistemes de comprovació d'estat de certificats per causes fora del control de l'EC-UR, aquesta realitza els seus millors esforços per assegurar que aquest servei es manté inactiu el mínim temps possible. L'EC-UR detalla en l'apartat 5.7.4 d'aquest document el màxim temps en què el servei ha de tornar a operar.

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

4.10.3. Altres funcions dels serveis

Sense estipulació addicional.

4.11. Acabament de la subscripció

La finalització de la subscripció no implica la revocació dels certificats que hagin estat emesos, sinó que aquests es poden utilitzar fins que expirin.

4.12. Dipòsit i recuperació de claus

4.12.1. Política i pràctiques de dipòsit i recuperació de claus

No es practica recuperació de claus per als certificats CEIXSA.

La recuperació de claus de la resta de certificats de xifrat la realitza CATCert a instància de l'EC-UR, que realitza mitjançant els seus procediments operatius. A aquest efecte, el procediment operatiu corresponent designa els rols que hauran d'intervenir en aquesta operació i que seran objecte de designació en l'entitat que realitzi l'operació

Per la realització de l'operació, un Operador de Paraules de Pas recuperarà el password d'accés a l'arxiu PKCS#12 que conté les claus pública i privada d'un certificat de xifrat (CPX, CEX). L'Operador de Paraules de Pas accedirà a la base de dades del servei KeyRecovery de la CA, buscarà el certificat corresponent i descarregarà el password d'accés a l'arxiu PKCS#12 a disc.

Un cop s'han recuperat de la base de dades del servei KeyRecovery de la CA tant l'arxiu PKCS#12 com el password, s'enviaran al Generador mitjançant email xifrat i signat. El Generador haurà d'inserir el certificat en una targeta nova en cas que l'antiga no estigués disponible (per pèrdua, robatori,...) o en la targeta antiga.

4.12.2. Política i pràctiques d'encapsulament i recuperació de claus de sessió

Sense estipulació addicional.

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

L'EC-UR 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 una anàlisi de gestió de risc per avaluar les necessàries mesures de seguretat.
- b. S'és responsable per a 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 se sustenta la prestació dels serveis.
- f. 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-UR disposa d'instal·lacions que protegeixen físicament la prestació, almenys, dels serveis de generació de certificats, de dispositius criptogràfics i de gestió del cicle de vida i del compromís causat per l'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-UR 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 del cicle de vida. La part de les instal·lacions compartides amb altres organitzacions es troba fora d'aquests perímetres.

L'EC-UR 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 del cicle de vida 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-UR.

Aquesta política de seguretat física i ambiental és revisada i aprovada pel CESCA 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-UR).

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 realitza serveis de preparació, inicialització i gestió de dispositius criptogràfics sense la presència física del seu posseïdor de claus (professor, personal administratiu i de serveis, 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-UR 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-UR on es duuguin 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.

La generació de claus criptogràfiques de l'EC-UR, 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 realitza serveis de preparació, inicialització i gestió de dispositius criptogràfics sense la presència física del seu posseïdor de claus (professor, personal administratiu i de serveis 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-UR 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-UR 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-UR compten amb sistemes automàtics de detecció i extinció d'incendis.

En concret, els dispositius criptogràfics i suports que emmagatzemen claus de les Entitats de Certificació han de disposar d'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 una 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.

Cal tenir 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 en paper com 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, aquesta se sotmet a un tractament físic de destrucció.

5.1.8. Còpia de seguretat fora de les instal·lacions

Periòdicament, l'EC-UR emmagatzema una còpia de seguretat dels sistemes d'informació en dependències físicament separades d'aquelles en les quals es troben els equips.

Es realitzarà una còpia de seguretat incremental diària i una còpia de seguretat setmanal.

En el moment de realitzar una sortida d'informació de les dependències s'adopten 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 xifrats).

5.2. Controls de procediments

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

El personal al servei de l'EC-UR realitza els procediments administratius i de gestió d'acord amb la política de seguretat de l'EC-UR. 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-UR.

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-UR 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-UR identifica i autèntica el personal abans d'accedir a la corresponent funció fiable.

5.2.4. Rols que requereixen separació de tasques

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

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

Les citades restriccions s'apliquen en tot cas:

- a. La persona que actua com a oficial de seguretat o com a operador de registre no pot ser auditor del sistema.
- b. La persona que actua com a administrador del sistema no pot ser oficial de seguretat ni auditor del sistema.
- c. Quan el registre és practicat per una Entitat de Registre amb presència física 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, serà imprescindible segregar els rols d'aprovador i generador (gaudint tots dos de la consideració d'operadors de registre).

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

5.3. Controls de personal

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

- Es manté la 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 infraestructures.
- S'és diligent i responsable en el tractament, manteniment i custòdia dels actius de la infraestructura 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 infraestructura, ni s'extreuen suports d'informació a nivells de seguretat inferiors.

- Es reporta al Responsable de Seguretat, tan bé com sigui possible, qualsevol incident que es consideri que afecta a la seguretat de la infraestructura, o limitar la qualitat del servei.
- S'utilitzen els actius de la infraestructura 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 infraestructura, programari o maquinari que no sigui expressament autoritzat per escrit pel responsable de sistemes d'informació.
- No s'accedeix voluntàriament, ni 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 de Certificació Digital
- el Responsable de l'EC-UR
- 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 Operadors de les Entitats de Registre.

En el CESCA, a més, es veu afectat el següent personal:

- qui fa les peticions dels certificats
- qui fa l'aprovació i validació de les peticions de certificats
- qui fa la generació / personalització de certificats
- qui custòdia les claus o tokens criptogràfics
- qui custòdia les claus o combinacions de seguretat d'accés a la sala d'operacions
- qui accedeix a informació classificada
- el personal de comunicacions i operacions
- el personal de seguretat (física i lògica) involucrats en l'operació
- el responsable del servei.

5.3.1.Requisits d'historial, qualificacions, experiència i autorització

L'EC-UR contracta 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-UR, especialment en relació amb procediments de personal de seguretat.

La qualificació i l'experiència poden suplir-se mitjançant una formació i una experiència professional apropiades.

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

5.3.2.Requisits de formació

L'EC-UR forma el personal en llocs fiables i de gestió, fins que aconseguixen 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

El CESCA (o les Entitats de Registre, quan pertoqui), a més, proporciona a 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 una instrucció periòdica en normes de seguretat, plans de contingència i gestió d'incidències.

5.3.3.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.

5.3.4.Seqüència i freqüència de rotació laboral

Sense estipulació addicional.

5.3.5.Sancions per accions no autoritzades

L'EC-UR 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.

5.3.6. Requisits de contractació de professionals

L'EC-UR contracta professionals per a qualsevol funció, fins i tot per a un lloc fiable, cas en el qual se sotmeten 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 certificació o de la DPC, són aplicats i completats pel tercer que realitza les funcions d'operació dels serveis de certificació; l'EC-UR 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-UR.

5.3.7. Subministrament de documentació al personal

L'EC-UR 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-UR 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-UR
- Intents no autoritzats d'accés als fitxers del sistema
- Generació de les claus de l'EC-UR
- Intents nuls de lectura i escriptura en un certificat i en el directori
- Esdeveniments relacionats amb el cicle de vida del certificat, com una sol·licitud, emissió, suspensió, habilitació, 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-UR 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-UR
- 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 seguretat 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 s'assegura 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 Certificació, 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 Certificació.

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-UR, 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. Anàlisi de vulnerabilitats

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

Les anàlisis de vulnerabilitat són executades, repassades i revisades per mitjà d'un examen d'aquests esdeveniments monitorats.

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

5.5. Arxiu d'informacions

L'EC-UR garanteix que tota la informació relativa als certificats es guarda durant un període de temps apropiat, segons l'establert 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-UR guarda registres de tots els esdeveniments que tinguin lloc durant el cicle de vida d'un certificat, incloent la renovació d'aquest.

L'EC-UR guarda un registre del següent:

Documents originals:

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

L'EC-UR guarda, en relació amb els certificats Extended Validation:

- LOG i pistes d'auditoria
- Documentació relativa a peticions, verificacions i revocacions de certificats Extended Validation

5.5.2. Període de conservació de registres

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

L'EC-UR guarda els registres especificats a la secció 5.5.1. en relació als certificats Extended Validation per un període de 7 anys, comptats des del moment de l'expedició del certificat.

5.5.3. Protecció de l'arxiu

L'EC-UR:

- 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. S'encarrega un tècnic de comunicacions del CESCA.

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 al CESCA. Aquestes còpies les guarda CATCert a les seves instal·lacions.

5.5.5. Requisits de segellat de cautela de data i hora

L'EC-UR 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-UR 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-UR tenen accés a les dades d'arxiu, sigui a les mateixes instal·lacions de l'EC-UR o en la seva ubicació externa.

5.6. Renovació de claus de les EC

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

5.7. Compromís de claus i recuperació de desastre

5.7.1. Procediment de gestió d'incidències i compromisos

L'EC-UR 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-UR 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-UR

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

En cas de compromís l'EC-UR:

- 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-UR ja no són vàlids.

5.7.4.Desastre sobre les instal·lacions

L'EC-UR 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 restauen 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-UR 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
- Publicació d'informació de revocació

La base de dades de recuperació de desastres utilitzada per l'EC-UR 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-UR tenen les mesures de seguretat físiques especificades en el Pla de Seguretat.

5.8. Acabament del servei

5.8.1.EC-UR

L'EC-UR assegura que les possibles interrupcions als subscriptors i a terceres parts són mínimes com a conseqüència del cessament dels serveis de l'EC-UR 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-UR executa, com a mínim, els següents procediments:

- Informa a tots els subscriptors i verificadors (no es requereix que l'EC-UR tingui alguna relació anterior amb terceres parts).
- Acaba tota autorització de subcontractacions que actuïn en nom de l'EC-UR 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.
- Destruïx les claus privades de l'EC-UR o les retira de l'ús.

En cas d'acabament del servei, l'EC-UR procedirà a:

- Notificació a les entitats afectades amb una antel·lació mínima de 2 mesos a la finalització efectiva del servei
- Transferència de les obligacions de l'EC-UR a altres persones, sota el seu consentiment
- Com es tracta l'estat de revocació dels certificats emesos que encara no han expirat.

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

5.8.2. Entitat de Registre

Les Entitats de Registre hauran de conservar i custodiar diligentment tota la informació generada en la seva activitat com a Entitat de Registre durant 15 anys després de finalitzar les activitats relacionades amb l'Entitat de Registre.

6. Controls de seguretat tècnica

L'EC-UR 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. Requisits per a tots els certificats

El parell de claus podrà ser generat pel futur subscriptor o per l'Entitat de Registre.

6.1.1.2. Informació per als certificats CIPISR, CPISR i CEISR

Les claus pública i privada dels certificats CIPISR, CPISR i CEISR 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).

6.1.1.3. Informació per als certificats CPIXSA

Les claus pública i privada dels certificats CPIXSA es generen per part de CATCert i s'envien al posseïdor de claus de forma segura. Aquestes claus no s'emmagatzemen, de manera que CATCert no respondrà per la pèrdua d'informació en cas de suspensió, revocació o expiració del certificat.

6.1.1.4. Informació per als certificats CPX i CEX

Les claus pública i privada dels certificats CPX i CEX es generen per part de l'Entitat de Certificació i són inserides al dispositiu de desxifrat.

Addicionalment una còpia de la clau privada s'emmagatzema a l'Entitat de Certificació.

6.1.1.5. Informació per als certificat CEIXSA

El parell de claus és generat pel futur posseïdor de claus.

6.1.1.6. Informació per als certificats CDS-1, CDS-1 EV i CDSCD-1

La clau pública dels certificats CDS-1, CDS-1 EV i CDSCD-1 es genera sota la seva responsabilitat, per part de l'Entitat de Registre. La clau privada la genera la Institució que sol·licita el certificat, i en cap cas s'envia al CESCA o a l'Entitat de Registre.

6.1.1.7. Informació per als certificats CDS-1 de seu electrònica EV

Les claus pública i privada dels certificats CDS-1 de seu electrònica EV es generen sota la seva responsabilitat, per part de l'Entitat de Registre, dins d'un dispositiu segur de creació de signatura electrònica. La clau pública dels certificats es genera sota la seva

responsabilitat, per part de l'Entitat de Registre i la clau privada la genera la Institució que sol·licita el certificat, i en cap cas s'envia al CESCA o a l'Entitat de Registre.

6.1.1.8. Informació per als certificats CDA-1 de segell electrònic

Les claus pública i privada dels certificats CDA-1 de segell electrònic es generen sota la seva responsabilitat, per part de l'Entitat de Registre, dins d'un dispositiu segur de creació de signatura electrònica. La clau pública dels certificats es genera sota la seva responsabilitat, per part de l'Entitat de Registre i la clau privada la genera la Institució que sol·licita el certificat, i en cap cas s'envia al CESCA o a l'Entitat de Registre.

6.1.1.9. Informació per als certificats CDP

Les claus pública i privada dels certificats CDP 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), o bé en programari.

6.1.2. Tramesa de la clau privada al subscriptor

6.1.2.1. Informació per als certificats CIPISR, CPISR, CEISR, CPX, CDP i CEX

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.

6.1.2.2. Informació per als certificats CEIXSA

La clau privada del subscriptor els és lliurada protegida en un contenidor criptogràfic segur, como el PKCS#12.

6.1.3. Tramesa de la clau pública a l'emissor del certificat

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

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

La clau de l'EC-UR i les claus de les Entitats de Certificació anteriors de la jerarquia pública de certificació de Catalunya estan a disposició 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 directori de l'EC-UR, en forma de certificat auto-signat, al costat d'una declaració referent a que la clau permet autenticar a l'EC-UR.

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-UR es publica en el directori de l'EC-UR, en forma de certificat CIC signat per CATCert.

Els usuaris accedeixen al directori per obtenir les claus públiques de l'EC-UR.

Adicionalment, 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 distribueixen als usuaris.

6.1.5. Mides de les claus

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

Les claus de tots els certificats emesos per l'EC-UR són de 2.048 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 la norma ETSI TS 102 176, que indica la qualitat dels algorismes de signatura electrònica.

6.1.8. Generació de les claus en aplicacions informàtiques o en béns d'equip

Els parells de claus de l'EC-UR són generats utilitzant maquinari criptogràfic que compleix els requisits establerts per l'especificació tècnica CEN CWA 14167 o equivalent.

Els parells de claus dels subscriptors de certificats reconeguts i de nivell alt, 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-UR o l'Entitat de Registre comprova l'autenticitat i el nivell de seguretat de les targetes o dispositius criptogràfics adquirits als proveïdors, abans d'autoritzar-ne l'ús.

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

6.1.9. Propòsits d'ús de les claus

L'EC-UR 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. Mòduls de protecció de la clau privada

6.2.1.1. Estàndards dels mòduls criptogràfics

Les claus privades de les Entitats de Certificació (tant de CATCert com de l'EC-UR) es protegeixen utilitzant maquinari criptogràfic que compleix els requisits establerts per l'especificació tècnica FIPS 140-2 Nivell 3 o superior.

Els parells de claus dels subscriptors de certificats de signatura electrònica reconeguda i de certificats de nivell alt estan protegits per targetes intel·ligents o altre maquinari que compleixen els requisits establerts per l'especificació tècnica CEN CWA 14169 o equivalent.

6.2.1.2. Cicle de vida de les targetes amb circuit integrat

Les targetes amb circuit integrat (altrament, targetes intel·ligents) es lliuren per l'emissió de cada nou certificat per l'Entitat de Registre, o bé directament per CATCert quan actua com a Entitat de Registre Virtual.

Per cada nova emissió o renovació dels certificats es lliura una targeta nova, és a dir, no es carrega certificats en targetes ja usades.

Quan CATCert detecti errors o defectes en les targetes, podrà retirar d'ofici les targetes afectades. En cas de detectar defectes o errors en casos puntuals, es substituirà la targeta afectada, prèvia revocació del certificat i s'emetrà un nou certificat que es lliurarà en una targeta nova sense cost addicional per al subscriptor.

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-UR 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-UR, i per al seu accés és necessària una persona addicional.

6.2.3. Dipòsit de la clau privada

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

Les claus privades dels certificats de xifrat sí es poden emmagatzemar a l'EC-UR.

6.2.4. Còpia de seguretat de la clau privada

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

6.2.5. Arxiu de la clau privada

La clau privada de l'EC-UR 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-UR.

Els controls de seguretat a aplicar en còpies de seguretat de l'EC-UR són d'igual o superior nivell a les que s'apliquen 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 de xifrat per garantir la recuperació de les dades.

6.2.6. Introducció de la clau privada en el mòdul criptogràfic

Les claus privades de l'EC-UR 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-UR.

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-UR obtenen o superen el nivell EAL 4 de Common Criteria (ISO 15408) o FIPS 140-2 nivell 3 amb els augments que determinen a l'especificació tècnica CEN CWA 14167 o equivalent.

Els mòduls dels subscriptors de certificats de signatura electrònica reconeguda i de certificats de nivell alt obtenen o superen el nivell EAL 4 de Common Criteria (ISO 15408) o FIPS 140-2 nivell 3 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-UR arxiva les seves claus públiques, d'acord amb l'establert a la secció 5.5.

6.3.2. Períodes d'utilització de les claus pública i privada

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

Com a excepció, la clau privada de desxifrat es pot continuar utilitzant 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-UR, quan el CESCA actua com a Entitat de Registre, facilita al subscriptor d'una banda, les dades d'activació de la targeta i, de l'altra, al cap de 3 dies, la targeta.

L'EC-UR, quan la Institució disposa d'una Entitat de Registre, facilita la targeta si s'escau, i quan el posseïdor es presenta a l'Entitat de Registre, se li creen o canvien les dades d'activació.

La Institució pot delegar en terceres entitats la creació i lliurament de les dades d'activació.

6.4.2. Protecció de les dades d'activació

6.4.2.1. Per a certificats personals i d'entitat

a) Quan el CESCA actua com a Entitat de Registre:

Per protegir al màxim les dades d'activació es distribueixen els elements dels certificats per dos canals diferents.

- En primer lloc, el responsable de l'Entitat de Registre lliura al posseïdor de claus el següent material:
 - Full de lliurament de posseïdor
 - Targeta amb els certificats
 - Programari necessari per utilitzar la targeta
 - Carta de lliurament de certificats.
- Al mateix temps, i per correu electrònic, s'envien al posseïdor de claus les dades d'activació del certificat.

D'aquesta forma s'aconsegueix que les dades d'activació estiguin distribuïdes separatament de la targeta i també en el temps.

b) Quan la Institució disposa d'Entitat de Registre:

Per protegir al màxim les dades d'activació, quan el posseïdor de claus es presenta físicament davant l'Entitat de Registre, 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 dispositiu CDS-1, CDS-1 EV, CDSCD-1, CDS-1 Seu electrònica de nivell mig EV i CDA-1 de segell electrònic de nivell alt

La distribució de les dades d'activació per als certificats de dispositiu CDS-1, CDS-1 EV, CDSCD-1, CDS-1 Seu electrònica de nivell mig EV i CDA-1 de segell electrònic de nivell alt, és diferent a la dels certificats personals (no té ni PIN ni PUK ni targeta), ja que la clau 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-UR 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-UR 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-UR, 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-UR està identificat i reconegut abans d'utilitzar aplicacions crítiques relacionades amb el cicle de vida del certificat.
- El personal de l'EC-UR 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-UR (per exemple, certificats o informació d'estat de revocació) compta amb un control d'accessos per a modificacions o esborrament de dades.

6.5.2. Avaluació del nivell de seguretat informàtica

Les aplicacions de EC i ER 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-UR 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-UR 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:

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

L'EC-UR 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 riscos 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 informàtics.

6.6.3. Avaluació del nivell de seguretat del cicle de vida

Sense estipulació adicional.

6.7. Controls de seguretat de xarxa

Es garanteix que l'accés a les diferents xarxes de l'EC-UR 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-UR.
- 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 publicada a la web de CATCert (<http://www.catcert.cat/>).

7.2. Perfil de la llista de revocació de certificats

Aquesta secció es troba publicada a la web de CATCert (<http://www.catcert.cat/>).

8. Auditoria de conformitat

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

8.1. Freqüència de l'auditoria de conformitat

L'EC-UR 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

El CESCA (exercint com a departament d'auditoria interna) o un Departament de la Institució que disposa d'Entitat de Registre, pot encarregar-se de realitzar l'auditoria de conformitat.

No obstant això, l'EC-UR 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 externes de conformitat executades per tercers estan realitzades per una entitat independent de l'EC-UR auditada. En cas d'auditoria interna, l'EC-UR s'ha d'assegurar que no existeix 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 s'obté l'informe de l'auditoria de compliment ja realitzada, l'EC-UR discuteix, amb l'entitat que ha executat l'auditoria, amb el CESCA i amb CATCert, les deficiències

trobades i desenvolupa i executa un pla correctiu que soluciona les esmentades deficiències.

Si l'EC-UR, 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-UR, de la forma com es descriu a la secció 4.9.
- Acabar el servei de l'EC-UR, de la forma com es descriu a la secció 5.8.

8.6. Tractament dels informes d'auditoria

L'EC-UR lliura els informes de resultats d'auditoria al CESCA i també 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

La Comissió de Seguiment i Control de l'EC-UR estableix les tarifes que aplica l'EC-UR, en la prestació dels seus serveis. Les tarifes es poden consultar al web de CATCert (<http://www.catcert.cat/tarifes/>).

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'estat dels certificats.

9.1.4. Tarifes d'altres serveis

Sense estipulació addicional.

9.1.5. Política de reintegrament

Ni l'EC-UR ni CATCert no practicaran reintegraments. En cas de productes defectuosos, es procedirà a substituir el producte defectuós per un altre en bon estat.

9.2. Capacitat financera

9.2.1. Assegurança de responsabilitat civil

CATCert 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. Aquesta assegurança cobreix les actuacions de CATCert com a prestador de serveis de certificació.

9.2.2. Altres actius

Sense estipulació addicional.

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

En cas d'ús incorrecte o no autoritzat dels certificats, ni CATCert ni l'EC-UR no actuaran com agent fiduciari front a subscriptors i terceres persones, que hauran de dirigir-se contra l'infractor de les condicions d'ús dels certificats establertes per CATCert i l'EC-UR.

9.3. Confidencialitat

9.3.1. Informacions confidencials

Les següents informacions són mantingudes com a confidencials per l'EC-UR:

- Informació de negoci subministrada pels seus proveïdors i altres persones amb qui CATCert o l'EC-UR tenen una obligació de guardar secret, establerta legalment o convencionalment.
- Registres de transaccions, incloent els registres complets i els registres d'auditoria de les transaccions.
- Registres d'auditoria interna i externa, creats i/o mantinguts per l'EC-UR i els seus auditors.
- Plans de continuïtat de negoci i d'emergència.
- Política i procediments de seguretat
- Documentació d'operacions i la resta de procediments d'operació, com ara arxiu, monitoratge i altres d'anàlegs.
- Tota altra informació identificada com a "Confidencial"

9.3.2. Informacions no confidencials

Les següents informacions no tenen caràcter confidencial:

- La Declaració de Pràctiques de Certificació de l'EC-UR
- Tota altra informació identificada com a "Pública"

9.3.3. Responsabilitat per la protecció d'informació confidencial

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

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

9.4. Protecció de dades personals

9.4.1. Política de Protecció de Dades Personals

CATCert desenvolupa una política de protecció de les dades personals, d'acord amb la Llei Orgànica 15/99, de 13 de desembre, de Protecció de Dades de Caràcter Personal (LOPD) i la normativa reglamentaria d'aplicació en matèria de protecció de dades de caràcter personal

Amb motiu de la prestació de serveis propis de certificació digital, esdevé responsable dels fitxers "Subscriptors de certificats" i "Persones físiques certificades", creats de conformitat amb la LOPD i notificats al Registre de l'Agència Catalana de Protecció de Dades.

L'estructura dels fitxers de dades de caràcter personal és la següent:

SUBSCRIPTORS DE CERTIFICATS:

- Dades identificatives del col·lectiu subscriptor: nom de l'entitat o de l'organisme que sol·licita els certificats, CIF, adreça postal completa, adreça electrònica, pàgina web.
- Dades identificatives de la persona que assumeix el rol de responsable del servei: nom, cognoms, DNI o equivalent, telèfon, fax, adreça postal, adreça electrònica.

PERSONES FÍSQUES CERTIFICADES:

- Dades identificatives: nom, cognoms i DNI o equivalent de la persona física certificada. Opcionalment, altres dades personals la inclusió de les quals sigui sol·licitada per la persona autoritzada, com el codi CIP de la Targeta Individual Sanitària.
- Dades de contacte: adreça postal completa a efectes de notificacions, així com l'adreça electrònica.
- Dades de l'entitat a la que presten els seus serveis (només en cas de certificats de classe 1 i de classe 2 de col·lectiu):
- Denominació de l'entitat, CIF, àrea d'adscripció política, orgànica, laboral o professional.

Les dades recollides i tractades pel prestador de serveis de certificació tenen la consideració legal de dades de nivell bàsic.

CATCert desenvolupa els procediments indicats en aquest document, que aplica en la prestació dels seus serveis, en els quals, 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 1720/2007, de 21 de desembre, que aprova el Reglament de Desenvolupament de la Llei Orgànica 15/1999 de Protecció de Dades de Caràcter Personal (RLOPD).

CATCert estableix les mesures de seguretat de caire tècnic i organitzatiu necessàries per donar compliment a les mesures de seguretat aplicables a fitxers i tractaments automatitzats del RLOPD i que es descriuen al Document de Seguretat LOPD. Amb caire merament informatiu es detallen a continuació les mesures aplicades, el precepte del RLOPD i la secció d'aquest document i de la Política General de Certificació de CATCert on es desenvolupen:

- a. Àmbit d'aplicació del document de seguretat amb especificació detallada dels recursos protegits (article 88 del RD 1720/2007) - secció 9.4
- b. Mesures, normes, procediments, regles i estàndards que garanteixin el nivell de seguretat exigít pel RD 1720/2007 - secció 9.4, i, en general, tots els controls tècnics de les seccions 5 i 6 de la Política General de Certificació de CATCert.
- c. Funcions i obligacions del personal (article 89 del RD 1720/2007) – secció 5.3.
- d. Registre d'incidències (article 90 del RD 1720/2007), procediment de notificació, gestió i resposta davant les incidències – secció 9.4.5
- e. Control d'accés (article 91 del RD 1720/2007) – seccions 5 i 6.
- f. Gestió de suports (article 92 del RD 1720/2007) – secció 5.
- g. Identificació i autenticació (article 93 del RD 1720/2007) – secció 5.2.

- h. Procediments de còpia de seguretat i recuperació de dades (article 94 del RD 1720/2007) - secció 5.5.

9.4.2. Dades de caràcter personal no disponibles a tercers

De conformitat amb allò 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.

Les dades de caràcter personal que hagin de ser incloses als certificats i al mecanisme indicat de comprovació de l'estat dels certificats són considerades dades de caràcter públic als efectes de la Llei de Signatura Electrònica. En aquest sentit, no seran considerades dades públiques disponibles a tercers:

- 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'Entitat de Certificació.
- Qualsevol altra dada de caràcter personal que no sigui susceptible de consulta, emmagatzemament o accés per tercers.

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

Les dades personal es tracten d'acord amb l'article 9 de la LOPD i garantint en tot cas la seguretat de les mateixes per evitar alteracions, pèrdues i accessos no autoritzats i d'acord amb les prescripcions establertes al Reial Decret 1720/2007, de 21 de desembre, que aprova el Reglament de Desenvolupament de la Llei Orgànica 15/1999 de Protecció de Dades de Caràcter Personal.

9.4.3. Dades de caràcter personal disponibles a tercers

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.

Aquestes dades de caràcter personal han d'estar disponibles per tercers per imperatiu legal ("dades públiques").

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'Entitat de Certificació.
- 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. L'adreça 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 Registre de l'Entitat de Certificació.

9.4.4.Responsabilitat corresponent a la protecció de les dades personals

CATCert, 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 en 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.

9.4.5.Gestió d'incidències relacionades amb les dades de caràcter personal

CATCert 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'Entitat de Certificació, a les seves instal·lacions, comunica immediatament per telèfon amb el Responsable de l'Àrea Tècnica de l'Entitat de Certificació, 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 a rebre la petició corresponent per correu electrònic signat digitalment, 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'Entitat de Certificació, protegit convenientment perquè només hi 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
- El procediment per a la recuperació
- La persona (i autorització) per a la recuperació
- Les dades restaurades.

9.4.6.Prestació del consentiment per al tractament de les dades personals

Per a la prestació del servei, CATCert necessita recollir i emmagatzemar certes informacions que comporta tractament de dades personals.

En l'expedició de certificats de classe 1 (amb càrrec) i de classe 2 (d'estudiant), aquestes dades són comunicades pels subscriptors, sense necessitat de consentiment dels afectats 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'article 6 de la LOPD.

CATCert informa els posseïdors de claus de l'obtenció de les seves dades personals de conformitat amb l'article 5 de la LOPD.

9.4.7.Comunicació de dades personals

CATCert només comunica les dades de caràcter personal a tercers en els casos legalment previstos.

En concret, CATCert està obligada a revelar la identitat dels signants quan ho 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.

CATCert dóna compliment a totes les prescripcions legals de conformitat amb la política de protecció de dades prevista a la secció 9.4.1.

Excepcionalment i per la situació prevista en la Política General de Certificació, que contempla el cas d'acabament de l'Entitat de Certificació, CATCert cedirà les dades personals per al supòsit de transferència de prestació del servei.

9.5. Drets de propietat intel·lectual

9.5.1. Propietat dels certificats i informació de revocació

CATCert és l'única entitat que gaudeix dels drets de propietat intel·lectual sobre els certificats que emet.

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

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

Addicionalment, els certificats emesos per l'EC-UR 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 Certificació i la 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-UR 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 dels subscriptors 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. Entitats de Certificació

9.6.1.1. Obligacions generals de l'EC-UR

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

- Determina la comunitat de subscriptors i verificadors de l'EC-UR.

- Aprova les polítiques de certificació i, si procedeix, les polítiques específiques de certificació.
- Aprova aquest document i la documentació contractual i reguladora dels serveis de certificació en la comunitat d'usuaris de l'EC-UR, d'acord amb el procediment previst en aquesta Declaració de Pràctiques de Certificació.
- Informa puntualment CATCert de totes les informacions relatives als canvis a realitzar, incidències en el servei, reclamacions, denúncies i inspeccions del servei.
- 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 subcontractades externament.
- Presta els seus serveis de certificació d'acord amb aquest document on es detallen almenys els continguts previstos a l'article 19 de la Llei 59/2003.
- Abans de l'emissió i lliurament del certificat al subscriptor, l'EC-UR l'informa dels aspectes previstos a l'article 18. b) de la Llei 59/2003, i dels següents aspectes:
 - Indicació de la política aplicable, amb indicació de si els certificats s'expedeixen al públic i de la necessitat d'utilització de dispositiu segur de creació de signatura.
 - Forma en que es garanteix la responsabilitat patrimonial per part de l'EC-UR.
 - L'EC-UR declara que té 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 els subscriptors, els posseïdors de claus i els verificadors mitjançant instruments jurídics apropiats a cada situació.
- Aquests instruments jurídics es transmeten electrònicament, estant 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 signatura.
 - Manifestació que la informació continguda al certificat és correcta, excepte notificació en contra pel subscriptor.
 - Consentiment per a la publicació del certificat en el directori 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-UR sense revocació de certificats vàlids.

- Límits d'ús del certificat, incloent els establerts 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-UR accepta o exclou la seva responsabilitat.
- Procediments aplicables de resolució de disputes.
- Llei aplicable i jurisdicció competent.
- La EC-UR 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, en concret:
 - L'EC-UR comprova per si mateixa o per mitjà d'una Entitat de Registre, la identitat i qualsevol altres circumstàncies personals dels sol·licitants dels certificats, d'acord amb l'establert a l'article 13 de la Llei 59/2003.
 - Quan el subscriptor del certificat de persona física (certificat de classe 1 i de classe 2 d'estudiant) és una persona jurídica, l'EC-UR comprova que el posseïdor de la clau es troba degudament autoritzat pel subscriptor.
- Compleix la resta d'obligacions contingudes a l'article 12 de la Llei 59/2003.

9.6.1.2. Informació per als certificats personals

L'EC-UR assumeix 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 a un document, que es considera inclòs de forma íntegra en la present política de certificat.

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

- Indicació de la política aplicable, amb indicació de 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 signatura.
- Certificació de serveis de l'EC-UR.
- Forma en què es garanteix la responsabilitat patrimonial de l'EC-UR.

9.6.1.3. Informació addicional per al CDS-1, CDS-1 EV, CDSCD-1 i CDS-1 Seu electrònica EV

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

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

9.6.1.4. Garanties ofertes a subscriptors i a verificadors

L'EC-UR, com a mínim, garanteix al subscriptor:

- 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 no hi hagi errors de fet en les informacions contingudes als certificats, coneguts o realitzats per l'EC-UR i, en el seu cas, per l'Entitat de Registre.
- c. Que no hi hagi errors de fet en les informacions contingudes als certificats, deguts a falta de diligència en la gestió de la sol·licitud de certificat o a la creació d'aquest.
- d. Que els certificats compleixin tots els requisits materials establerts en aquesta DPC.
- e. Que els serveis de revocació i l'ús del directori compleixin tots els requisits materials establerts en la DPC.

L'EC-UR, 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 directori, 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

Adicionalment, l'EC-UR garanteix al subscriptor i al verificador :

- 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.
- 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.
- La responsabilitat de l'EC-UR, amb els límits que s'estableixin.

9.6.2. Obligacions i altres compromisos de les Entitats de Registre

En relació amb la gestió del cicle de vida dels certificats, l'Entitat de Registre s'obliga a complir el següent:

- a. Actua exclusivament en relació amb persones vinculades a l'Entitat de Registre.
- b. Nomena com a operadors de l'autoritat de registre, a quatre o a més dels seus treballadors, i comunica a CATCert les dades corresponents a aquestes persones per a l'emissió dels certificats d'operador corresponents. 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 l'EC-UR la revocació del certificat d'operador corresponent.
- c. Valida i aprova les sol·licituds de certificats i, tot seguit, genera els certificats per als posseïdors de claus, d'acord amb els procediments i instruments tècnics establerts

per l'EC-UR, el contingut d'aquest document i la documentació d'operacions de l'EC-UR.

- d. Si l'Entitat de Registre 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.
- e. Verifica, quan sigui necessari, qualsevol atribut específic del posseïdor de claus, i registra un justificant acreditatiu de la informació.
- f. Realitza o tramita les sol·licituds de suspensió, habilitació, revocació i renovació de certificats, d'acord amb els procediments i els instruments tècnics establerts per l'EC-UR, d'acord amb aquest document, i la documentació d'operacions de l'EC-UR.
- g. Emmagatzema els registres, ja sigui en paper, ja sigui 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-UR.
- h. Aporta la justificació documental necessària per al registre d'usuaris i per a la posterior emissió de certificats per part de l'EC-UR o l'Entitat de Registre.
- 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. Garanties ofertes a subscriptors i verificadors

9.6.3.1. Garantia de CATCert pels serveis de certificació digital

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

CATCert únicament garanteix que:

- a) Els certificats de signatura electrònica contenen tota la informació exigida per la Llei 59/2003, de 19 de desembre.
- b) No ha originat ni ha introduït declaracions falses o errònies 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) Queda vinculada pels procediments operatius, d'arxiu i de seguretat descrits en aquest document i al conveni entre CATCert, el CESCA, i l'EC-UR

9.6.3.2. 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

La EC-UR obliga al subscriptor a:

- a. Facilitar a l'EC-UR informació completa i adequada, en especial pel que respecta al procediment de registre.
- b. Manifestar el seu consentiment previ a l'emissió i lliurament d'un certificat.
- c. 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.
- d. Utilitzar el certificat d'acord amb l'establert a la secció 1.4.
- e. Notificar a l'EC-UR, sense endarreriments injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu segur de creació de signatura.
- f. Notificar l'EC-UR i qualsevol persona que el subscriptor cregui que pugui confiar en el certificat, sense endarreriments 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 signatura) o per qualsevol altra causa.
 - c) Les inexactituds o canvis en el contingut del certificat que conegui o pugués conèixer el subscriptor.
- g. Deixar d'utilitzar la clau privada transcorregut el període indicat a la secció corresponent.
- h. No monitorar, manipular o realitzar actes d'enginyeria inversa sobre la implantació tècnica de la Jerarquia de l'Agència Catalana de Certificació, sense permís previ per escrit.
- i. No comprometre intencionadament la seguretat de la Jerarquia de l'Agència Catalana de Certificació.

9.6.4.1.2. Informacions específiques per als certificats de signatura electrònica reconeguda

L'EC-UR obliga el subscriptor a:

- a. Utilitzar el parell de claus exclusivament per a signatures electròniques i conforme a qualsevol altra limitació que li sigui notificada.
- b. Reconèixer que aquestes signatures electròniques són signatures electròniques equivalents a signatures 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 signatura, a fi d'evitar usos no autoritzats.
- d. Notificar a l'EC-UR, sense endarreriments injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu segur de creació de signatura.
- e. El subscriptor que generi les seves pròpies claus, , 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 signatura.
 - 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

L'EC-UR obliga al subscriptor, mitjançant el corresponent instrument jurídic, a garantir que:

- a. Totes les manifestacions realitzades a la sol·licitud són correctes.
- b. Totes les informacions subministrades pel subscriptor que es troben 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 signatura.
- 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

L'EC-UR obliga el subscriptor, mitjançant el corresponent instrument jurídic, a garantir que el subscriptor 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-UR 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 monitorar, 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 signatures electròniques produïdes per certificats reconeguts de signatura reconeguda són signatures electròniques equivalents a signatures 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-UR obliga al verificador, mitjançant el corresponent instrument jurídic, a manifestar:

- a. Que disposa de suficient informació per prendre una decisió informada per confiar o no amb el certificat.
- b. Que és l'únic responsable de confiar o no en la informació continguda al certificat.
- c. Que 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 directori

L'EC-UR pot delegar algunes funcions en el directori 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 directori 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 directori

L'EC-UR té la responsabilitat civil del directori de certificació quan sigui operat per una tercera entitat.

9.7. Renúncies de garanties

9.7.1. Rebuig de garanties de l'EC-UR

L'EC-UR pot rebutjar 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 l'EC-UR

L'EC-UR 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 signatura, així com de xifrat o desxifrat).

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

A aquest efecte, l'EC-UR vetlla perquè, almenys els requisits continguts a les seccions Obligacions i Responsabilitat civil, Auditoria de conformitat, i Confidencialitat, continuïn

vigents després de l'acabament de la política de certificació i dels instruments jurídics que vinculen l'EC-UR amb subscriptors i verificadors.

CATCert determinarà un Pla de Continuitat de Negoci. Aquest Pla de Continuitat de Negoci establirà les obligacions que assumeix CATCert en cas de cessació d'activitats, dirigides a mantenir en vigència els certificats emesos fins la seva expiració i l'ús i custòdia de tota la informació generada per CATCert en la seva activitat de prestador de serveis de certificació tals com còpies de seguretat, logs i documents de tota mena, independentment del suport en què han estat generats o emmagatzemats. A tal efecte, CATCert s'assegura de que es genera una còpia de seguretat amb periodicitat, com a previsió complementària de l'activitat corrent i igualment de l'assegurament de la continuïtat de negoci.

9.11. Notificacions

L'EC-UR 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

El procediment per a la modificació d'aquesta DPC està establert en la secció 1.5.4 d'aquesta DPC. En un procés de modificació s'haurà de tenir en compte:

- La modificació ha d'estar justificada des del punt de vista tècnic, legal o comercial.
- La modificació proposada per l'EC-UR 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.
-

9.12.2. Termini i mecanismes per a notificacions

Les modificacions d'aquest document es notifiquen a CATCert, pels mitjans legalment establerts en el termini d'un mes.

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-UR estableix, als seus instruments jurídics amb subscriptors i 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-UR, quan sigui aplicable aquesta circumstància.

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

9.13.2. Jurisdicció competent

L'EC-UR estableix, als seus instruments jurídics vinculants amb subscriptors i 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-UR tingui la consideració d'Administració Pública es té en compte la legislació administrativa que resulti aplicable.

9.14. Llei aplicable

L'EC-UR estableix, als seus instruments jurídics amb subscriptors i 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-UR 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-UR 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-UR estableix, als seus instruments jurídics vinculants amb subscriptors i 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-UR.

9.16.3. Divisibilitat

L'EC-UR 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.

Per al cas que, com a causa als articles 7 i 8 de la Llei 7/1998 sobre condicions generals de la contractació, es consideren no incorporades al contracte, o nul·les algunes o qualsevol de les clàusules indicades, la no incorporació referida o nul·litat no determina la ineficàcia total del contracte, si aquest pogués subsistir sense les clàusules indicades.

9.16.4. Aplicacions

Sense estipulació addicional.

9.16.5. Altres clàusules

Sense estipulació addicional.

Annex I.

Projecte:	Informe modificació del document DPC EC-UR
Entitat de destí:	Agència Catalana de Certificació
Codi de referència:	Revisió 1r semestre 2011
Versió:	Canvis de la v5. 4 a la v5.5 en català i en castellà
Data de l'edició:	30/06/2011

Control de versions DPC EC-UR 1r semestre 2011

Versió	Parts que canvien	Descripció del canvi	Autor del canvi	Data del canvi
5.5	1.1.1.2, 1.1.1.4, 1.2.2, 6.1	Introducció CPIXSA Càrrec EP, CDS-1 EV i característiques CDS-1 Seu electrònica EV (nivell mig i alt)	Oficina de Polítiques	30/06/2011
5.5	4.4.1.1	Adaptació del procediment de lliurament al refactoring	Oficina de Polítiques	30/06/2011
5.5	4.9.1.6	Inclusió de causa de revocació per als CDP	Oficina de Polítiques	30/06/2011
5.5	5.8.1	Modificació de les condicions per a l'acabament del servei	Oficina de Polítiques	30/06/2011
5.5	5.8.2	Custòdia de documentació per les Entitats de Registre	Oficina de Polítiques	30/06/2011
5.5	6.1.5	Adaptació mides claus	Oficina de Polítiques	30/06/2011
5.5	6.4.2	Adaptació del procediment de lliurament de les dades d'activació al	Oficina de Polítiques	30/06/2011

		procediment (refactoring)		
5.5			Oficina de Polítiques	30/06/2011
5.5	9.6	Reestructuració de la informació relativa a les obligacions de l'EC i les ER	Oficina de Polítiques	30/06/2011