



**Agència Catalana
de Certificació**

Declaració de Pràctiques de Certificació

Entitat de Certificació de les Administracions Locals

(EC-AL)

Referència: D1111 N-DPC-EC-AL v3r5 cat

Versió: 3.6

Data: 03/12/2010

Índex

1. Introducció.....	8
1.1 Presentació	8
1.1.1. Tipus i classes de certificats	8
1.1.2. Relació entre la Declaració de pràctiques de certificació i altres documents.....	14
1.2 Nom del document i identificació.....	15
1.2.1. Identificació d'aquest document.....	15
1.2.2. Identificació de polítiques de certificació cobertes per aquesta DPC.....	15
1.3 Comunitat d'usuaris de certificats	17
1.3.1. Prestadors de serveis de certificació.....	17
1.3.2. Entitat de Certificació Arrel	17
1.3.3. EC-AL	18
1.3.4. Entitats de Registre.....	18
1.3.5. Usuaris finals.....	19
1.4 Ús dels certificats	20
1.4.1. Usos típics dels certificats	20
1.4.2. Aplicacions prohibides	28
1.5. Administració de la Declaració de Pràctiques.	30
1.5.1. Organització que administra l'especificació.....	30
1.5.2. Dades de contacte de l'organització.....	30
1.5.3. Persona que determina la conformitat d'una DPC amb la política.....	30
1.5.4. Procediment d'aprovació.....	31
2. Publicació d'informació i directori de certificats	32
2.1. Directori de certificats.....	32
2.2. Publicació d'informació de l'EC-AL.....	32
2.3. Freqüència de publicació	32
2.4. Control d'accés	33
3. Identificació i autenticació.....	34
3.1. Gestió de noms.....	34
3.1.1. Tipus de noms	34
3.1.2. Significat dels noms	34
3.1.3. Utilització d'anònims i pseudònims	34
3.1.4. Interpretació de formats de noms	34
3.1.5. Unicitat dels noms	34
3.1.6. Resolució de conflictes relatius a noms.....	34
3.2. Validació inicial de la identitat.....	35
3.2.1. Prova de possessió de clau privada	35
3.2.2. Autenticació de la identitat d'una Organització	36
3.2.3. Autenticació de la identitat d'una persona física.....	37
3.2.4. Informació no verificada	38

3.3. Identificació i autenticació de sol·licituds de renovació	38
3.3.1. Validació per a la renovació rutinària de certificats	38
3.3.2. Validació per a la renovació de certificats després de la revocació	38
4. Característiques d'operació del cicle de vida dels certificats	39
4.1 Sol·licitud d'emissió de certificat.....	39
4.1.1 Legitimació per a sol·licitar l'emissió	39
4.1.2. Procediment d'alta; Responsabilitats	40
4.2. Processament de la sol·licitud de certificació	40
4.2.1. Requisits generals per a tots els certificats	40
4.2.2. Requisits específics per al CEIXSA	41
4.2.3. Informacions addicionals per al CDS, el CDSCD y el CDS-1 de Seu electrònica	41
4.2.4. Requisits específics per al CIPISR	42
4.2.5. Altres certificats	42
4.3. Emissió de certificat	42
4.3.1. Accions de l'EC-AL durant el procés d'emissió	42
4.3.2. Notificació de l'emissió al subscriptor	43
4.4. Acceptació del certificat	43
4.4.1. Responsabilitats de l'Entitat de Registre	43
4.4.2. Conducta que constitueix acceptació del certificat.....	45
4.4.3. Publicació del certificat	45
4.4.4. Notificació de l'emissió a tercers	45
4.5. Ús del parell de claus i del certificat	45
4.5.1. Ús del parell de claus pels posseïdors de claus i ús dels certificats pels subscriptors ...	45
4.5.2. Ús pel tercer que confia en certificats	47
4.6. Renovació de certificats sense renovació de claus	48
4.7. Renovació de certificats amb renovació de claus.....	48
4.8. Modificació de certificats.....	48
4.9. Revocació i suspensió de certificats.....	48
4.9.1. Causes de revocació de certificats	48
4.9.2. Legitimació per a sol·licitar la revocació.....	50
4.9.3. Procediments de sol·licitud de revocació	50
4.9.4. Període temporal de sol·licitud de revocació.....	51
4.9.5. Període màxim de processament de la sol·licitud de revocació.....	51
4.9.6. Obligació de consulta de informació de revocació de certificats	51
4.9.7. Freqüència d'emissió de llistes de revocació de certificats (LRCs).....	51
4.9.8. Període màxim de publicació de LRCs	51
4.9.9. Disponibilitat de serveis de comprovació d'estat de certificats.....	51
4.9.10. Obligació de consulta de serveis de comprovació d'estat de certificats.....	52
4.9.11. Altres formes d'informació de revocació de certificats.....	52
4.9.12. Requisits especials en cas de compromís de la clau privada	52
4.9.13. Causes de suspensió de certificats	52
4.9.14. Legitimació per sol·licitar la suspensió.....	53
4.9.15. Procediments de sol·licitud de suspensió	53
4.9.16. Període màxim de suspensió	54
4.9.17. Habilitació d'un certificat suspès	54

4.10.	Serveis de comprovació d'estat de certificats.....	54
4.10.1.	Característiques d'operació dels serveis.....	54
4.10.2.	Disponibilitat dels serveis.....	54
4.10.3.	Altres funcions dels serveis.....	55
4.11.	Acabament de la subscripció	55
4.12.	Dipòsit i recuperació de claus.....	55
4.12.1.	Política i pràctiques de dipòsit i recuperació de claus	55
4.12.2.	Política i pràctiques d'encapsulament i recuperació de claus de sessió	55
5.	Controls de seguretat física, de gestió i d'operacions.....	56
5.1.	Controls de seguretat física	56
5.1.1.	Localització i construcció de les instal·lacions.....	57
5.1.2.	Accés físic	57
5.1.3.	Electricitat i aire condicionat.....	57
5.1.4.	Exposició a l'aigua	57
5.1.5.	Advertència i protecció d'incendis.....	58
5.1.6.	Emmagatzematge de suports	58
5.1.7.	Tractament de residus.....	58
5.1.8.	Còpia de seguretat fora de les instal·lacions.....	58
5.2.	Controls de procediments	58
5.2.1.	Funcions fiables.....	59
5.2.2.	Nombre de persones per tasca	59
5.2.3.	Identificació i autenticació per a cada funció	59
5.2.4.	Rols que requereixen separació de tasques.....	59
5.3.	Controls de personal	60
5.3.1.	Requisits d'historial, qualificacions, experiència i autorització	61
5.3.2.	Requisits de formació.....	61
5.3.3.	Requisits i freqüència d'actualització formativa	62
5.3.4.	Seqüència i freqüència de rotació laboral.....	62
5.3.5.	Sancions per accions no autoritzades	62
5.3.6.	Requisits de contractació de professionals	62
5.3.7.	Subministrament de documentació al personal	62
5.4.	Procediments d'auditoria de seguretat.....	62
5.4.1.	Tipus d'esdeveniments registrats	62
5.4.2.	Freqüència de tractament de registres d'auditoria	63
5.4.3.	Període de conservació de registres d'auditoria	63
5.4.4.	Protecció dels registres d'auditoria	63
5.4.5.	Procediments de còpies de seguretat	63
5.4.6.	Localització del sistema d'acumulació de registres d'auditoria	64
5.4.7.	Notificació de l'esdeveniment d'auditoria al causant de l'esdeveniment	64
5.4.8.	Anàlisi de vulnerabilitats	64
5.5.	Arxiu d'informacions	64
5.5.1.	Tipus d'esdeveniments registrats	64
5.5.2.	Període de conservació de registres.....	65
5.5.3.	Protecció de l'arxiu	65
5.5.4.	Procediments de còpia de suport	65
5.5.5.	Requisits de segellat de cautela de data i hora.....	65

5.5.6.	Localització del sistema d'arxiu	65
5.5.7.	Procediments d'obtenció i verificació d'informació d'arxiu	65
5.6.	Renovació de claus.....	65
5.7.	Compromís de claus i recuperació de desastre.....	66
5.7.1.	Procediment de gestió d'incidències i compromisos.....	66
5.7.2.	Corrupció de recursos, aplicacions o dades.....	66
5.7.3.	Compromís de la clau privada de l'EC-AL	66
5.7.4.	Desastre sobre les instal·lacions	66
5.8.	Acabament del servei	66
5.8.1.	EC-AL	66
5.8.2.	Entitat de Registre	67
6.	Controls de seguretat tècnica	68
6.1.	Generació i instal·lació del parell de claus	68
6.1.1.	Generació del parell de claus.....	68
6.1.2.	Tramesa de la clau privada al subscriptor	69
6.1.3.	Enviament de la clau pública a l'emissor del certificat	69
6.1.4.	Distribució de la clau pública del Prestador de Serveis de Certificació	69
6.1.5.	Mides de claus	69
6.1.6.	Generació de paràmetres de clau pública	69
6.1.7.	Comprovació de qualitat de paràmetres de clau pública	69
6.1.8.	Generació de claus en aplicacions informàtiques o en bens d'equip.....	69
6.1.9.	Propòsits d'ús de claus	70
6.2.	Protecció de la clau privada	70
6.2.1.	Mòduls de protecció de la clau privada	70
6.2.2.	Control per més d'una persona (n de m) sobre la clau privada	70
6.2.3.	Dipòsit de la clau privada	71
6.2.4.	Còpia de seguretat de la clau privada	71
6.2.5.	Arxiu de la clau privada	71
6.2.6.	Introducció de la clau privada en el mòdul criptogràfic	71
6.2.7.	Emmagatzematge de la clau privada en el mòdul criptogràfic	71
6.2.8.	Mètode d'activació de la clau privada	71
6.2.9.	Mètode de desactivació de la clau privada	71
6.2.10.	Mètode de destrucció de la clau privada	71
6.2.11.	Classificació dels mòduls criptogràfics	71
6.3.	Altres aspectes de gestió del parell de claus	72
6.3.1.	Arxiu de la clau pública.....	72
6.3.2.	Períodes d'utilització de les claus pública i privada.....	72
6.4.	Dades d'activació	72
6.4.1.	Generació i instal·lació de les dades d'activació	72
6.4.2.	Protecció de les dades d'activació	72
6.4.3.	Altres aspectes de les dades d'activació	73
6.5.	Controls de seguretat informàtica	73
6.5.1.	Requisits tècnics específics de seguretat informàtica.....	73
6.5.2.	Avaluació del nivell de seguretat informàtica	73
6.6.	Controls tècnics del cicle de vida.....	74

6.6.1.	Controls de desenvolupament de sistemes	74
6.6.2.	Controls de gestió de seguretat	74
6.6.3.	Avaluació del nivell de seguretat del cicle de vida	74
6.7.	Controls de seguretat de xarxa.....	74
6.8.	Segell de temps.....	74
7.	<i>Perfils de certificats i llistes de certificats revocats</i>	75
7.1.	Perfil de certificat	75
7.2.	Perfil de la llista de revocació de certificats	75
8.	<i>Auditoria de conformitat</i>	76
8.1.	Freqüència de l'auditoria de conformitat.....	76
8.2.	Identificació i qualificació de l'auditor	76
8.3.	Relació de l'auditor amb l'entitat auditada.....	76
8.4.	Relació d'elements objecte d'auditoria.....	76
8.5.	Accions a emprendre com a resultat d'una falta de conformitat	76
8.6.	Tractament dels informes d'auditoria	77
9.	<i>Requisits comercials i legals</i>	78
9.1.	Tarifes.....	78
9.1.1.	Tarifa d'emissió o renovació de certificats	78
9.1.2.	Tarifa d'accés a certificats.....	78
9.1.3.	Tarifa d'accés a informació d'estat de certificat	78
9.1.4.	Tarifes d'altres serveis.....	78
9.1.5.	Política de reintegrament	78
9.2.	Capacitat financera	78
9.2.1.	Assegurança de responsabilitat civil	78
9.2.2.	Altres actius.....	78
9.2.3.	Cobertura d'assegurament per a subscriptors i tercers que confien en certificats	78
9.3.	Confidencialitat	78
9.3.1.	Informacions confidencials	78
9.3.2.	Informacions no confidencials	79
9.3.3.	Responsabilitat per la protecció d'informació confidencial	79
9.4.	Protecció de dades personals	79
9.4.1.	Política de Protecció de Dades Personals	79
9.4.2.	Dades de caràcter personal no disponibles a tercers.....	80
9.4.3.	Dades de caràcter personal disponibles a tercers.....	81
9.4.4.	Responsabilitat corresponent a la protecció de les dades personals	82
9.4.5.	Gestió d'incidències relacionades amb les dades de caràcter personal	82
9.4.6.	Prestació del consentiment per al tractament de les dades personals	83
9.4.7.	Comunicació de dades personals.....	83
9.5.	Drets de propietat intel·lectual	83
9.5.1.	Propietat dels certificats i informació de revocació.....	83
9.5.2.	Propietat de la Política de Certificació i Declaració de Pràctiques de Certificació	84

9.5.3.	Propietat de la informació relativa a noms	84
9.5.4.	Propietat de claus.....	84
9.6.	Obligacions i responsabilitat civil	84
9.6.1.	Entitats de Certificació	84
9.6.2.	Entitats de Registre.....	87
9.6.3.	Subscriptors	89
9.6.4.	Verificadors	91
9.6.5.	Altres participants.....	91
9.7.	Renúncies de garanties.....	92
9.7.1.	Rebuig de garanties de la EC-AL	92
9.8.	Limitacions de responsabilitat	92
9.8.1.	Limitacions de responsabilitat de la EC-AL.....	92
9.8.2.	Cas fortuït i força major	92
9.9.	Indemnitzacions.....	92
9.9.1.	Clàusula d'indemnitat de subscriptor	92
9.9.2.	Clàusula d'indemnitat de verificador	92
9.10.	Termini i acabament	92
9.10.1.	Termini	92
9.10.2.	Finalització	92
9.10.3.	Supervivència	92
9.11.	Notificacions.....	93
9.12.	Modificacions	93
9.12.1.	Procediment per a les modificacions	93
9.12.2.	Termini i mecanismes per a notificacions	93
9.12.3.	Circumstàncies en les que un OID ha de ser canviat.....	93
9.13.	Resolució de conflictes.....	93
9.13.1.	Resolució extrajudicial de conflictes.....	93
9.13.2.	Jurisdicció competent	94
9.14.	Llei aplicable	94
9.15.	Conformitat amb la llei aplicable.....	94
9.16.	Clàusules diverses.....	94
9.16.1.	Acord íntegre	94
9.16.2.	Subrogació.....	94
9.16.3.	Divisibilitat	94
9.16.4.	Aplicacions	95
9.16.5.	Altres clàusules.....	95

ANNEX I. Control de canvis

1. Introducció

1.1 Presentació

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-AL 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 en certificats de classe 1 actua habitualment en representació o per compte d'una persona jurídica.
- Certificats d'entitat, caracteritzats pel fet que el subscriptor del certificat i, d'acord amb la llei, el signant, és una persona jurídica, que actua per mitjà d'un posseïdor de claus.
- Certificats de dispositiu, caracteritzats pel fet que no hi ha un posseïdor de la clau privada sinó que són utilitzats per dispositius informàtics, que en certificats de classe 1 es troben sota la responsabilitat d'una persona jurídica.

Els certificats de classe 1 són, per tant, certificats corporatius, caracteritzats pel fet que la persona física té una vinculació amb el subscriptor del certificat, que és una persona jurídica. Habitualment el subscriptor actua com a entitat de registre dels certificats, encara que no és estrictament necessari.

La resta de certificats són certificats de classe 2. 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-AL emet els següents tipus de certificats personals:

1. Certificats personals d'identitat i de signatura electrònica reconeguda de classe 1 (CPISR-1), que identifiquen la persona que els posseeix, la seva organització subscriptora, 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.
2. 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.
3. 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.
4. 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.

5. Certificats personals de xifrat de classe 1 (CPX-1), que identifiquen la persona que els posseeix, la seva organització subscriptora, i que s'utilitzen per produir o rebre missatges o documents confidencials, en qualsevol format. No permeten la signatura electrònica de missatges de dades.
6. 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 o documents confidencials en qualsevol format. No permeten la signatura electrònica de missatges de dades.
7. 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 o documents confidencials en qualsevol format. No permeten la signatura electrònica de missatges de dades.
8. Certificats personals d'identificació i de signatura avançada de classe 1 (CPISA-1), 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 personal d'identificació i signatura reconeguda de classe 1 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 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.

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, en nom d'Ajuntaments, Consells Comarcals, Diputacions, etc, així com dels ens dependents i vinculats als anteriors (en endavant "les Institucions").

El certificat personal d'identificació i de signatura electrònica reconeguda de classe 1 amb càrrec (CPISR-1 Càrrec), 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 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 escrita, sinó només la identificació del posseïdor de claus, en nom de la Institució.

El certificat personal 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 dóna 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 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 escrita, sinó només la identificació del posseïdor de claus, en nom de la Institució.

El certificat personal de xifrat de classe 1 (CPX-1) 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 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 1 amb càrrec (CPX-1 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. A més inclouen una manifestació relativa a la categoria de personal i càrrec del posseïdor de claus, que ha estat comprovada abans d'emetre el certificat, i és correcta. 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 escrita, sinó només la identificació del posseïdor de claus, en nom de la Institució.

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 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 d'identificació i signatura avançada de classe 1 (CPISA-1) 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".

1.1.1.3. Certificats d'entitat

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

1. Certificats d'entitat d'identificació i 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 permet que Institucions públiques i privades, corporacions de dret públic i persones jurídico-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.
2. 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 permet que Institucions públiques i privades, corporacions de dret públic i persones jurídico-públiques (col·lectivament anomenades "entitats") puguin xifrar o rebre missatges de dades confidencials, en qualsevol format.
3. 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 permet que Institucions públiques i privades, corporacions de dret públic i persones jurídico-públiques (col·lectivament anomenades "entitats") signin documents electrònicament, missatges d'autenticació (confirmació de la identitat) i d'accés segur a sistemes informàtics i puguin xifrar i rebre missatges de dades i documents confidencials, en qualsevol format.

Adicionalment, en funció dels requeriments tècnics y 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.

1.1.1.4. Certificats de dispositiu

L'EC-AL 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 de seu electrònica nivell mig de classe 1 (CDS-1 Seu electrònica nivell mig), 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.ex. 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 mig es lliurarà en suport programari.

- Certificat de dispositiu de seu electrònica nivell alt de classe 1 (CDS-1 Seu electrònica nivell alt), 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 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 contemplen 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 (CDA), que emmagatzemat en un servidor i requerit per una aplicació, signa documents o missatges.
- 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.ex. 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 contemplen 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 programari o de signatura d'aplicacions informàtiques de classe 1 (CDP-1), que serveix per signar electrònicament les aplicacions informàtiques o programari a transmetre a través d'Internet. Així, els usuaris finals poden signar elements com applets, scripts, executables, etc.

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-AL.

L'EC-AL 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-AL 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-AL".

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

1.3.6.1.4.1.15096.1.2.5

1.2.2. Identificació de polítiques de certificació cobertes per aquesta DPC

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

- **CIPISR** – Certificat d'infraestructura d'operador, emès per la EC-AL
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 la EC-AL
CIC-1. OID: 1.3.6.1.4.1.15096.1.3.1.11
CIC-2. OID: 1.3.6.1.4.1.15096.1.3.1.12
CIC-3. OID: 1.3.6.1.4.1.15096.1.3.1.13
- **CIDS-1** – Certificat de infraestructura de servidor segur, emès per la EC-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.17
- **CIDA-1** – Certificat d'infraestructura d'aplicació, emès per la EC-AL
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 la EC-AL
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 la EC-AL
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 la EC-AL
Classe 1. 1.3.6.1.4.1.15096.1.3.1.111
- **CPIISR-1** - Certificat personal d'identificació i signatura electrònica reconeguda, emès per l'EC-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.81
- **CPIISR-1 amb Càrrec** – Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec, emès per la EC-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.2.5.

-
- **CPISR-1 amb Càrrec Ús**- Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec per a ús concret, emès per l'EC-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.3.2
 - **CPISR-2 amb Càrrec** – Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec, emès per la EC-AL
Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.82.3.5.
 - **CPX-1** - Certificat personal de xifrat , emès per l'EC-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.41
 - **CPX Càrrec** - Certificat personal de xifrat amb càrrec, emès per l'EC-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.41.1.5
Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.42.3.5
 - **CPISA-1** – Certificat personal d'identificació amb signatura electrònica reconeguda, emès per l'EC-AL
OID: 1.3.6.1.4.1.15096.1.3.1.83
 - **CEISR-1** – Certificat d'entitat d'identificació amb signatura electrònica reconeguda, emès per l'EC-AL.
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.121.2
 - **CEX-1** – Certificat d'entitat de xifrat emès per l'EC-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.131.2
 - **CEIXSA-1** – Certificats d'entitat d'identificació, xifrat i signatura electrònica avançada emès per l'EC-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.161.2
 - **CDS-1** - Certificat de dispositiu servidor segur, emès per l'EC-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51
 - **CDS-1 Seu electrònica nivell mig** – Certificat de dispositiu servidor segur, seu electrònica nivell mig, emès per l'EC-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.2
 - **CDS-1 Seu electrònica nivell alt** – Certificat de dispositiu servidor segur, seu electrònica nivell alt, emès per l'EC-AL
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-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.91
 - **CDA-1 segell electrònic nivell mig** - Certificat de dispositiu d'aplicació digitalment assegurada, segell electrònic nivell mig, emès per l'EC-AL
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.91.1
 - **CDA-1 segell electrònic nivell alt** - Certificat de dispositiu d'aplicació digitalment assegurada, segell electrònic nivell alt, emès per l'EC-AL
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-AL
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-AL
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-AL no s'expedeixen al públic, sinó a les entitats, al personal i als dispositius de les Institucions (Ajuntaments, Consells Comarcals, Diputacions, així com Organismes Autònoms i Empreses Públiques de les anteriors)

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>), que té la finalitat d'integrar altres entitats de

certificació al sistema públic català de certificació mitjançant la vinculació tècnica de les autoritats de certificació corresponents.

1.3.3. EC-AL

L'EC-AL és l'Entitat de Certificació de les Administracions Locals, vinculada a la jerarquia d'entitats de certificació de les entitats públiques de Catalunya, que emet els certificats indicats en el punt 1.1.1.

1.3.4. Entitats de Registre

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

Els diversos Organismes, Departaments i Empreses Públiques de les Administracions Locals, poden actuar com a Entitats de Registre.

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 d'aquesta Política General de Certificació i de la Declaració de Pràctiques de Certificació.

En certificats de classe 1, l'Entitat de Registre i el subscriptor podran ser la mateixa organització i, en conseqüència, habitualment l'Entitat de Registre podrà actuar també com a sol·licitant del certificat.

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

Existeixen tres tipus d'Entitats de Registre:

- 1) Les Entitats de Registre Internes, operades per una institució subscriptora de certificats de classe 1.
- 2) Les Entitats de Registre Virtuals, corresponents a institucions, que són subscriptores de certificats y que han delegat el registre a CATCert o a Entitats de Registre Col·laboradores.
- 3) Les Entitats de Registre Col·laboradores, que assisteixen a les institucions subscriptores de certificats de classe 1 (que en tot cas actuen com a Entitat de Registre Virtual) en el procés d'emissió dels certificats, i que col·laboren amb Entitats de Certificació Vinculades en el procés d'emissió dels certificats de classe 2.

Les institucions, per ser Entitats de Registre Internes, s'hauran de dissenyar i implantar els corresponents components i procediments tècnics, jurídics i de seguretat, referents al cicle de vida dels certificats que emetin.

Aquests components i procediments seran prèviament aprovats per l'Entitat de Certificació.

1.3.5. Usuaris finals

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

- Els sol·licitants de certificats
- Els subscriptors o titulars de certificats
- Els posseïdors de claus
- Els verificadors de signatures, de segells i de certificats

1.3.5.1. 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.

1.3.5.2. 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.

1.3.5.3. 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.

1.3.5.4. Usuaris de certificats

Els usuaris dels certificats són els verificadors.

1.3.5.5. 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.

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, un determinat càrrec 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, establint 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. Els certificats d'infraestructura personal d'identificació i signatura reconeguda (CIPISR)

Els certificats d'infraestructura d'identificació i signatura reconeguda són certificats reconeguts 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 reconeguda 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 CIPISR 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 CIPISR 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 CIPISR són certificat 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 Internes o Col·laboradores per aprovar i generar certificats, o per revocar-los, o pel servei d'atenció a usuaris per suspendre certificats.

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

Els CIPISR 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'infraestructura 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, CIPISR, CIDS, CIDA, CIO, CIV, CIT, CIPISR, CPX, CEX, CDS i CDA.
- 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 (CPISR-1), Certificats personals d'identificació i signatura electrònica reconeguda de classe 1 amb càrrec (CPISR-1 càrrec), 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, els certificats personals d'identificació i signatura reconeguda de classe 1 amb càrrec, 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 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 que donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

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

Per aquest motiu, aquests certificats garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten la generació de la signatura electrònica reconeguda; és a dir, la signatura electrònica avançada que es basa en un

certificat reconegut i que ha estat generada utilitzant un dispositiu segur, per la qual cosa, d'acord amb el que estableix l'article 3 de la Llei 59/2003, de 19 de desembre, s'equipara a la signatura escrita per efecte legal, sense necessitat de complir cap altre requeriment addicional.

Aquests certificats inclouen una manifestació relativa a la categoria de personal i càrrec del posseïdor de claus, que han estat comprovats abans d'emetre el certificat, i són correctes, quan ho prevegi una política específica.

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 distribuïda, basada en presentació de la credencial
- Autenticació en sistemes de control d'accés, de sistema operatiu o centralitzats.

1.4.1.2.2. Certificats personals de xifrat de classe 1 (CPX-1)

El certificat personal de xifrat 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, i que dóna 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 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. El posseïdor de la clau utilitza la seva clau privada per desxifrar el missatge.

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

La clau privada d'aquests certificats 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.

1.4.1.2.3. Certificats personals de xifrat de classe 1 amb càrrec (CPX-1 càrrec)

El certificat personal de xifrat de classe 1 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 dóna 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 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.

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

El certificat personals 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 dóna 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.

1.4.1.2.5. 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 que dóna 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 d'identificació i signatura avançada de classe 1 (CPISA-1)

El certificat personal d'identificació i signatura avançada 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.

1.4.1.3. Certificats d'entitat

1.4.1.3.1. Certificats d'Entitat d'Identificació i 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 que donen compliment al dispost 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; això 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 escrita 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 de entitat de xifrat de classe 1 són certificats reconeguts, no emesos al públic, que s'expedeixen a subscriptors i s'utilitzen exclusivament per xifrar o rebre missatges de

dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, utilitzant la clau pública del subscriptor indicada al CEX.

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

El posseïdor de la clau utilitzarà 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 que 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 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 CDS 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

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

1.4.1.4.2. Certificat de dispositiu de seu electrònica de classe 1 (CDS-1 Seu electrònica nivell mig i alt)

Els CDS-1 Seu electrònica s'emeten a les Institucions, 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 es poden 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.

Es distingeixen dos certificats:

- El certificat de nivell mig, lliurat en suport programari, i 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.

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

Els CDSCD s'emeten a 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.

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

Els CDA s'emeten a persones jurídiques responsables de l'operació d'aplicacions informàtiques que s'identifiquen digitalment, que signa electrònicament webservices o altres protocols i que rep documents i missatges xifrats.

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

1.4.1.4.5. 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 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 altres. Es distingeixen dos certificats:

- El certificat de nivell mig, lliurat en suport programari, 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 contemplen 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.

1.4.1.4.6. 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, i que garanteixen la identitat de la persona responsable i l'origen i la integritat del programari signat.

1.4.2. Aplicacions prohibides

1.4.2.1. Informacions per a tots els tipus de certificats

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

Certificats d'infraestructura Certificat d'infraestructura personal d'identificació i 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

1.4.2.3.1. Certificats personals d'identificació i signatura electrònica reconeguda

Els certificats CIPISR-1, CIPISR-1 amb Càrrec, CIPISR-1 amb Càrrec ús, i CIPISR-2 amb Càrrec 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).
- Xifrar ni desxifrar missatges o documents.

1.4.2.3.2. Certificats personals de xifrat

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

1.4.2.4 Certificats d'entitat

1.4.2.4.1 Certificats d'entitat d'identificació i signatura electrònica reconeguda

Els certificats CEISR 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).
- Xifrar ni desxifrar missatges o documents.
-

1.4.2.4.2 Certificats d'entitat de xifrat

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

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

Els CEIXSA 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).

Realitzar signatura electrònica reconeguda de documents

1.4.2.5. Certificats de dispositiu

1.4.2.5.1 Certificats de dispositiu de servidor segur

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

1.4.2.5.2. Certificat de dispositiu de servidor segur seu electrònica

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

1.4.2.5.3 Certificats de dispositiu d'Aplicació digitalment assegurada

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

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

1.4.2.5.4 Certificats de dispositiu d'aplicació digitalment assegurada segell electrònic
Els CDA-1 segell no es poden utilitzar per a la realització d'actes manuals.

1.4.2.5.5 Certificats de dispositiu de signatura de programari
Sense estipulació addicional

1.5. Administració de la Declaració de Pràctiques.

1.5.1. Organització que administra l'especificació

CATCert - Agència Catalana de Certificació

Passatge de la Concepció, 11

08008 - Barcelona

Telèfon: 93 272 26 00

Fax: 93 272 25 39

Correu electrònic: info@catcert.net

Telèfon assistència:

902 901 080

1.5.2 Dades de contacte de l'organització

CATCert - Agència Catalana de Certificació

Passatge de la Concepció, 11

08008 - Barcelona

Telèfon: 93 272 26 00

Fax: 93 272 25 39

Correu electrònic: info@catcert.net

Telèfon assistència:

902 901 080

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

CATCert - Agència Catalana de Certificació

Passatge de la Concepció, 11
08008 - Barcelona
Telèfon: 93 272 26 00
Fax: 93 272 25 39
Correu electrònic: info@catcert.net
Telèfon assistència:
902 901 080

1.5.4 Procediment d'aprovació

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

Es preveu, d'aquesta manera, el procediment de modificació d'especificació del servei i el procediment de publicació d'especificacions de servei. Les modificacions finals de la DPC són aprovades per CATCert una vegada comprovat el compliment dels requisits establerts en les seccions corresponents d'aquesta DPC.

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-AL, 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-AL

L'EC-AL publica les següents informacions, en el seu web:

- 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-AL, a través del dipòsit.

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

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

2.3. Freqüència de publicació

La informació de l'EC-AL 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-AL, podent ser consultada, per causa raonada pels interessats.

2.4. Control d'accés

L'EC-AL no limita l'accés de lectura a les informacions del Directori, 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-AL 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 Directori.

3.1.1.2. Perfils dels certificats

Els perfils dels certificats emesos per l'EC-AL es publiquen al web de CATCert (<http://www.catcert.cat/>).

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

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-AL 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-AL es reserva el dret de refusar una sol·licitud de certificat a causa de conflicte de nom.

En certificats d'organització, 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.

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

- En cas de nacionals espanyols, el DNI del subscriptor.
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 subscriptor.
V.gr.: francès (C) = ES; (SN) = NIE
V.gr.: argentí (C) = ES; (SN) = NIE
- En cas d'estrangers nacionals d'Estat que són part de l'Acord Schengen i que no disposen de NIE, el document nacional d'identitat del país d'origen o de procedència o passaport vigent del subscriptor.
V.gr.: italià (C) = IT; (SN) = IT-Document nacional de identitat
- En cas d'estrangers nacionals d'Estat que no són part de l'Acord Schengen i que no disposen de NIE, el Passaport ordinari, diplomàtic, oficial o de servei, del subscriptor 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 subscriptor és nacional, separat per un guió, de conformitat amb els paràmetres establerts per la norma ISO 3166 Codes (Countries).

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-AL 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-AL 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.

3.2.2.1.1. Subscriptors de certificats

3.2.2.1.1.1. 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.

3.2.2.1.1.2. Requisits per a certificats de classe 2

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

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

- 1) Obtenció d'informació sobre l'organització, d'un proveïdor extern de serveis d'aquesta naturalesa, a discreció de l'Entitat de Certificació, que prèviament haurà d'aprovar el proveïdor extern.
- 2) Comprovació de documentació justificativa aportada pel sol·licitant, sobre els següents extrems:
 - a) Nom legal complet de l'organització
 - b) Estat legal de l'organització
 - c) Nombre d'identificació fiscal
 - d) Dades d'identificació registral.

3.2.2.1.1.3. Requisits específics per als CDS i CDSCD

En el cas dels certificats de dispositiu de servidor segur i de controlador de domini, 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.

3.2.2.1.1.4. 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.

3.2.2.1.1.5. Requisits específics per al CDP

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

L'operador de l'Entitat de Registre introdueix la informació que identifica el posseïdor de claus, que troba a l'expedient associat a la petició de subscripció.

En el cas que la Institució no disposi d'informació actualitzada del posseïdor de claus, es comprova la identitat personalment o s'utilitzen sistemes que proporcionin garanties equivalents a la identificació amb presència física del futur posseïdor de claus, i es grava una justificació acreditativa dels següents elements:

- Nom complet
- Data de naixement
- 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, etc.).

3.2.3.2. Validació dels elements d'identificació

La informació d'identificació de posseïdors de claus de certificats de Classe 1 és vàlida 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.

Es pot ocupar un proveïdor corporatiu d'informació de recursos humans per a aquesta tasca. La informació del posseïdor registrada la Institució 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 o professional, 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 Institució es responsabilitza que tota la informació inclosa a la sol·licitud del certificat sigui exacta, completa per a la finalitat del certificat. No obstant això no es pot responsabilitzar que es tingui dret al seu ús (per exemple dret a utilitzar cert nom a l'adreça electrònica o la legitimitat en l'ocupació d'un servidor web).

3.3. Identificació i autenticació de sol·licituds de renovació

3.3.1. Validació per a la renovació rutinària de certificats

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

4.1 Sol·licitud d'emissió de certificat

4.1.1 Legitimació per a sol·licitar l'emissió

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

La sol·licitud és, el primer pas que ha de fer el subscriptor per aconseguir els certificats per al seu personal.

En el cas de les administracions públiques, la sol·licitud es trametrà:

- A través de les seves Entitats de Registre T-CAT
- Directament CATCert, de forma supletòria en cas que l'ens no tingui cap entitat de registre assignada. En aquest cas CATCert actuarà com a Entitat de Registre T-CAT.

Aquesta sol·licitud requereix la tramesa d'un document amb la informació exacta i comprovada (certificat) de les persones o dispositius per a les que es demana el certificat. Aquesta sol·licitud se signa per 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 lliurarà a l'Entitat de registre telemàticament. Excepcionalment podrà ser lliurada en suport paper o mitjançant correu electrònic signat i xifrat, per les causes següents:

- Que per raons tècniques o d'aplicatiu informàtic no pugui ser usuari d'aquest per raó de la seva naturalesa jurídica,
- Que sigui la primera vegada que demani certificats digitals per tractar-se d'un ens de nova creació.

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 s'ha de gestionar pel responsable del sistema de certificació digital, encarregat de l'Entitat de Registre, directament a CATCert.

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

4.1.2. Procediment d'alta; Responsabilitats

La Institució és la responsable de realitzar el procediment d'alta.

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

CATCert posa a disposició del subscriptor la documentació (model de formulari) necessària a fi de sol·licitar certificats, a través de l'aplicació telemàtica, o bé en format paper per a les primeres emissions dels ens nous.

4.2. Processament de la sol·licitud de certificació

4.2.1. Requisits generals per a tots els certificats

Per tal que un ens públic pugui sol·licitar certificats telemàticament, prèviament cal donar-se d'alta en l'aplicació telemàtica corresponent. En cas que sigui la primera vegada que es demanen certificats o que l'ens no en sigui usuari de l'aplicació telemàtica, haurà de fer servir el canal alternatiu establert en aquest apartat.

El procediment a seguir per a sol·licitar certificats digitals és el següent:

1. Lliurament de la Fitxa del Subscriptor.

Per tal que un ens públic pugui sol·licitar certificats, prèviament cal que faci arribar la Fitxa del Subscriptor a CATCert telemàticament. Per poder fer ús d'aquesta opció cal disposar de certificats digitals per a tots els rols que intervenen en el procés de sol·licitud (sol·licitant, certificador i responsable del servei).

En cas que sigui la primera vegada que es demanen certificats o que l'ens no en sigui usuari, haurà de fer servir el canal alternatiu següent:

- Descàrrega de la fitxa del subscriptor

- Enviament de la fitxa signada digitalment a l'adreça: scd@catcert.cat, o bé signada manuscritament per correu ordinari a l'adreça que es recull a la secció 1.5.2 d'aquest document.

El lliurament d'aquesta documentació només cal realitzar-lo junt amb la primera sol·licitud de certificats o en cas que es produeixin canvis en la mateixa.

2. Obtenció dels certificats

Cal fer la sol·licitud dels certificats telemàticament. Per poder fer ús d'aquesta opció cal disposar de certificats digitals per a tots els rols que intervenen en el procés de sol·licitud (sol·licitant, certificador i responsable del servei).

Quan la sol·licitud hagi estat realitzada telemàticament, un cop completada la sol·licitud, cal signar-la digitalment pel sol·licitant, i en els certificats personals, també pel certificador. Un

cop signada pel sol·licitant, automàticament s'envia un correu electrònic al certificador de l'ens avisant-lo que ha de verificar les dades de la sol·licitud del certificat.

El certificador és la persona de l'ens amb capacitat per justificar documentalment les dades del titular del certificat a emetre, per exemple, el/la secretari/ària, el/la responsable de recursos humans, etc.

El certificador de l'ens obre la sol·licitud signada anteriorment i, si comprova que les dades són correctes, la signa digitalment finalitzant el procés de sol·licitud. En aquest moment es fa automàticament l'assentament del registre de sortida de l'ens i d'entrada a la seva entitat de registre T-CAT.

L'EC-AL rep directament les dades de la sol·licitud en format digital i les carrega a l'aplicació de generació de certificats. Un cop el certificat s'ha generat, s'envia a l'ens subscriptor.

Si la sol·licitud no ha estat realitzada telemàticament, cal sol·licitar prèviament els certificats pel canal alternatiu següent:

- Descàrrega del model de sol·licitud i el certificat de dades corresponent.
- Enviament dels documents signats digitalment a l'adreça: scd@catcert.cat, o bé signats manuscritament per correu ordinari a l'adreça que es recull a la secció 1.5.2 d'aquest document.

El termini de lliurament dels certificats és d'un màxim de 21 dies naturals a partir de la data d'arribada de la documentació correctament emplenada i signada. En cas que s'opti pel servei urgent, el lliurament serà de 4 dies laborables.

4.2.2. Requisits específics per al CEIXSA

Una vegada aprovada la sol·licitud, la EC-AL rep l'autorització de l'Entitat de Registre, recupera la corresponent sol·licitud, l'emmagatzema en l'estructura de certificats, sent signada per la EC-AL, 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 CDSCD y el CDS-1 de Seu electrònica

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-AL 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 Virtual.

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 certificat¹
- En cas que l'Entitat de Certificació aporti el dispositiu segur de creació de signatura, emprar un procediment de gestió de dispositius segurs de creació de signatura que assegurí que l'esmentat dispositiu és lliurat de forma segura al posseïdor de claus².
- 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 suport³.
- 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

4.2.5. Altres certificats

Les sol·licituds realitzades són processades i es realitza la validació. En el cas que tot sigui correcte, es tramita la sol·licitud a l'Entitat de Registre. 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-AL 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, l'EC-AL 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 certificada⁵
- 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,

¹ Llei 59/2003: Art. 20.1 b)

² TS 101 456: 7.3.3 c); TS 102042: 7.3.3 c)

³ Llei 59/2003: Art. 20.1 d)

⁴ TS 101 456: 7.3.3, amb referència a D 99/93: Annex II g);

⁵ TS 101 456: 7.3.3 b)

en cas de certificats individuals, o al posseïdor de claus en cas de certificats d'organització⁶.

- 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 cas⁷.
- 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 certificat⁸.
- En cas de que l'Entitat de Certificació aporti 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 claus⁹.
- 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 suport¹⁰.
- 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.¹¹

4.3.2. Notificació de l'emissió al subscriptor

CATCert 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

4.4.1.1. Per a Certificats personals

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

CATCert també crea els corresponents codis PIN i PUK de les targetes (dispositius criptogràfics) on s'allotgen el parell de claus i el certificat.

⁶ TS 101 456: 7.3.3 c)

⁷ TS 101 456: 7.3.3 e)

⁸ art. 20,1,b) Llei 59/2003

⁹ TS 101 456: 7.3.3 c)

¹⁰ Llei 59/2003: 20.1.d)

¹¹ TS 101 456: 7.3.3, en referència a D 99/93: Annex II g); art. 20,1,e) Llei 59/2003

L'EC-AL 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.

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

Paral·lelament, CATCert trametrà al responsable de l'Entitat de Registre virtual de l'ens subscriptor la/les targeta/tes amb el certificat sol·licitats per correu ordinari.

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-AL 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 al 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.

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 dels certificats 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 poden utilitzar-se 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 al CDS

Els CDS 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.

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-AL.

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

De les dades incloses al certificat només es poden modificar les dades personals (nom, cognoms, i adreça). Per realitzar les modificacions, l'Entitat de Registre podrà requerir l'acreditació de les condicions justificatives de la modificació.

4.9. Revocació i suspensió de certificats.

4.9.1. Causes de revocació de certificats

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

1. Circumstàncies que afecten la informació continguda al certificat
 - Modificació d'alguna de les dades contingudes al certificat.
 - Descobriment que alguna de les dades contingudes a la sol·licitud de certificat és incorrecta.
 - Descobriment que alguna de les dades contingudes al certificat és incorrecte.
2. Circumstàncies que afecten a la seguretat de la clau o del certificat
 - Compromís de la clau privada o de la infraestructura o sistemes de l'EC-AL, sempre que afecti la confiança en els certificats emesos a partir d'aquest incident.
 - Infracció, per a l'EC-AL, dels requisits previstos en els procediments de gestió de certificats.
 - Compromís o sospita de compromís de la seguretat de la clau o del certificat del subscriptor.
 - Accés o utilització no autoritzat, per un tercer, de la clau privada del subscriptor.

-
- L'ús irregular del certificat pel subscriptor o falta de diligència en la custòdia de la clau privada.
3. Circumstàncies que afecten el dispositiu criptogràfic
- Compromís o sospita de compromís de la seguretat del dispositiu criptogràfic.
 - Pèrdua o inutilització del dispositiu criptogràfic.
 - Accés no autoritzat, per un tercer, a les dades d'activació del subscriptor.
4. Circumstàncies que afecten el subscriptor o el posseïdor de claus
- Final de la relació entre l'EC-AL i el subscriptor.
 - Modificació o extinció de la relació jurídica subjacent o causa que va provocar l'emissió del certificat al subscriptor.
 - Infracció per al sol·licitant del certificat dels requisits preestablerts per a la sol·licitud d'aquest.
 - Infracció per al subscriptor de les seves obligacions, responsabilitat i garanties, establertes a l'instrument jurídic corresponent de l'EC-AL.
 - La incapacitat sobrevinguda o la mort del subscriptor.
 - 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-AL, 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).

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

L'instrument jurídic que vincula l'EC-AL 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 o l'Entitat de Registre que va sol·licitar l'emissió del certificat.

4.9.3. Procediments de sol·licitud de revocació

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

La sol·licitud de revocació ha de ser tramitada telemàticament. Excepcionalment es podrà tramitar 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-AL, el certificat que se sol·licita revocar, i 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 la Institució 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-AL no pot reactivar el certificat, una vegada revocat.

Nota: Un certificat revocat no es pot tornar a utilitzar; 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 de informació de revocació de certificats

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

Un mètode pel qual es verifica l'estat dels certificats és consultant la llista de revocació de certificats o LRC més recent emesa per l'EC-AL. L'estat de vigència també es pot comprovar online mitjançant el protocol OCSP.

L'EC-AL 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-AL 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.

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 es publiquen immediatament en el web de CATCert.

4.9.9. Disponibilitat de serveis de comprovació d'estat de certificats

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

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

El verificador que no utilitza LRC per comprovar la validesa d'un certificat, ho pot fer en el Dipòsit de l'EC-AL, al qual s'haurà de poder accedir directament a través de la pàgina web de CATCert.

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

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

L'EC-AL 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-AL 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 número 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 retornarà 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-AL és notificat, en la mesura possible, a tots els participants en la jerarquia pública de certificació de Catalunya, 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 la documentació requerida a la sol·licitud de revocació sigui suficient però no es pugui identificar raonablement el posseïdor de claus.

- Quan la documentació requerida a la sol·licitud de revocació no sigui suficient, encara que es pugui identificar raonablement el posseïdor de claus
- Quan la documentació requerida a la sol·licitud de revocació no sigui suficient i tampoc no permetin identificar raonablement el posseïdor de claus.
- Si el subscriptor no utilitza el certificat durant un període prolongat de temps, conegut prèviament.
- Si se sospita el compromís d'una clau, fins que aquest sigui confirmat. En aquest cas, l'EC-AL 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, les Entitats de Registre, que van emetre el certificat o les Entitats de Registre Col·laboradores.

4.9.15. Procediments de sol·licitud de suspensió

La suspensió dels certificats 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 mitjà d'una trucada 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 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-AL directament, a través del component LRA o des de la web de consulta avançada de certificats.

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 la Institució 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 Dipòsit de Certificació de CATCert instal·lades per als verificadors.

4.10.2. Disponibilitat dels serveis

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

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

L'EC-AL 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

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

4.12. Dipòsit i recuperació de claus

4.12.1. Política i pràctiques de dipòsit i recuperació de claus

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-AL, 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). 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-AL 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 dóna 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-AL 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, del compromís causat per accés no autoritzat als sistemes o a les dades.

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

Aquesta política de seguretat física i ambiental és revisada i aprovada 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-AL).

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

5.1.2. Accés físic

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

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

5.1.3. Electricitat i aire condicionat

Els equips informàtics de l'EC-AL 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-AL 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-AL compten amb sistemes automàtics de detecció i extinció d'incendis.

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

5.1.6. Emmagatzematge de suports

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

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

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

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 paper com de magnètics, es realitza mitjançant mecanismes que garanteixen la impossibilitat de recuperació de la informació.

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

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

5.1.8. Còpia de seguretat fora de les instal·lacions

Periòdicament, l'EC-AL emmagatzema una còpia de seguretat backup 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-AL garanteix que els seus sistemes s'operen de forma segura, i per això estableix i implanta procediments per a les funcions que afecten la provisió dels seus serveis.

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

Les funcions fiables inclouen:

- Personal responsable de la seguretat
- 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-AL, 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-AL identifica i autèntica el personal abans d'accedir a la corresponent funció fiable.

5.2.4. Rols que requereixen separació de tasques

L'EC-AL 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.

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

5.3. Controls de personal

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

- Es manté confidencialitat de la informació, posant els mitjans necessaris i mantenint una actitud adequada en el desenvolupament de les seves funcions i, fora de l'àmbit laboral en allò referent a la seguretat de les 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, el més aviat 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 no s'elimina o altera informació no destinada a la seva persona o perfil professional.

El personal afectat per aquesta normativa és:

- el Responsable del Servei de Certificació Digital
- el Responsable de l'EC-AL
- 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.

A CATCert, 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 custodia les claus o tokens criptogràfics
 - qui custodia 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-AL ocupa personal qualificat i amb l'experiència necessària per a la prestació dels serveis oferts, en l'àmbit de la signatura electrònica i els procediments de seguretat i de gestió adequats.

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

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

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

5.3.2. Requisits de formació

L'EC-AL 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

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

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

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

5.3.7. Subministrament de documentació al personal

L'EC-AL 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-AL 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-AL

-
- Intents no autoritzats d'accés als fitxers del sistema
 - Generació de les claus de l'EC-AL
 - 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-AL 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-AL
- 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 a la setmana 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 elèctrics, es protegeixen de lectures, modificacions, esborraments o qualsevol altre tipus de manipulació no autoritzada usant controls d'accés lògic i físic.

5.4.5. Procediments de còpies de seguretat

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

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

-
- Es guarden en armaris ignífugs
 - Només persones autoritzades disposen d'accés a les còpies de seguretat
 - Les còpies estan identificades
 - Si un material ha contingut còpies de seguretat (disquets, dvd's...) i es vol reutilitzar 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-AL, compost pels registres de l'aplicació, pels de xarxa i pels 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 monitoritzar les vulnerabilitats del sistema.

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

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

5.5. Arxiu d'informacions

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

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

L'EC-AL 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-AL:

- 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 de CATCert.

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

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

5.5.5. Requisits de segellat de cautela de data i hora

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

5.6. Renovació de claus

Els certificats de l'EC-AL renovats es comuniquen als usuaris finals, mitjançant la seva publicació en la pàgina web de CATCert.

5.7. Compromís de claus i recuperació de desastre

5.7.1. Procediment de gestió d'incidències i compromisos

L'EC-AL 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-AL 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-AL

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

En cas de compromís l'EC-AL:

- 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-AL ja no són vàlids.

5.7.4. Desastre sobre les instal·lacions

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

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

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

5.8. Acabament del servei

5.8.1. EC-AL

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

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

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

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

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

5.8.2. Entitat de Registre

Sense estipulació addicional.

6. Controls de seguretat tècnica

L'EC-AL 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 CPISR i CEISR

Les claus pública i privada dels certificats CPISR i CEISR es generen per part de CATCert 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 CPX i CEX

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

Adicionalment una còpia de la clau privada s'emmagatzema a CATCert.

6.1.1.4. Informació per als certificats CEIXSA

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

6.1.1.5. Informació per als certificats CDS i CDSCD

La clau pública dels certificats CDS i CDSCD es genera sota la seva responsabilitat, per part de l'Entitat de Registre. La clau privada la genera la Institució.

6.1.1.5. Informació per als certificats CDS-1 Seu electrònica

Les claus pública i privada dels certificats CDS-1 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 a l'Entitat de Registre Interna.

6.1.1.6. Informació per als certificats CDA-1 Segell electrònic

Les claus pública i privada dels certificats CDA-1 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, en el cas dels CDA-1 de nivell alt, i en cap s'envia a l'Entitat de Registre Interna.

6.1.1.7. 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 CPISR, CEISR, CDP, CPX 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 certificat CEIXSA

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

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

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

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

La clau de l'EC-AL 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-AL, en forma de certificat auto-signat, al costat d'una declaració referent a que la clau permet autenticar a l'EC-AL.

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

Els usuaris accedeixen al Directori per obtenir les claus públiques de l'EC-AL.

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 distribueix als usuaris.

6.1.5. Mides de claus

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

Les claus dels subscriptors de certificats de signatura electrònica i dels certificats de nivell alt l'EC-AL són almenys de 1.024 bits.

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

6.1.6. Generació de paràmetres de clau pública

Sense estipulació addicional.

6.1.7. Comprovació de qualitat de paràmetres de clau pública

Es realitza d'acord amb l'informe especial de l' ETSI TS 101 276, que indica la qualitat dels algorismes de signatura electrònica.

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

Els parells de claus de l'EC-AL 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 certificats 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-AL 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 poden realitzar-se mitjançant aplicacions informàtiques.

6.1.9. Propòsits d'ús de claus

L'EC-AL 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-AL) 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 reconeguts 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 Col·laboradora o Interna, 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-AL requereix el concurs 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-AL, i per al seu accés és necessària una persona addicional.

6.2.3. Dipòsit de la clau privada

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

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

6.2.4. Còpia de seguretat de la clau privada

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

6.2.5. Arxiu de la clau privada

La clau privada de l'EC-AL compta amb una còpia de seguretat realitzada, emmagatzemada, i recuperada quan convingui, 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-AL.

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

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

No s'emmagatzemen còpies de les claus privades dels certificats, excepte en el cas dels certificats CPX, per garantir la recuperació de les dades.

6.2.6. Introducció de la clau privada en el mòdul criptogràfic

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

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-AL.

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

Els mòduls dels subscriptors de certificats reconeguts i 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-AL 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 les determinades 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-AL facilita al subscriptor, d'una banda una targeta, i al cap de 3 dies les dades d'activació de la targeta.

6.4.2. Protecció de les dades d'activació

6.4.2.1. Per a certificats personals i d'entitat.

Per protegir al màxim les dades d'activació CATCert s'encarrega de generar dues trameses diferents.

- En la primera tramesa, s'envia a l'adreça del subscriptor però a l'atenció del posseïdor de claus (i només aquest últim pot obrir-lo), el següent material:
 - Sobre cec amb els codi PIN i PUK, només en el cas que sigui la primera sol·licitud.
- Al cap de 3 dies, es produeix la segona tramesa, també a l'adreça del subscriptor, i amb el següent material:
 - Full de lliurament de posseïdor
 - Full de lliurament de subscriptor
 - Targeta amb els certificats
 - Programari necessari per utilitzar la targeta
 - Carta de lliurament de certificats.

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

6.4.2.2. Per a certificats de dispositiu CDS, CDSCD, CDS-1 Seu electrònica de nivell mig i CDA-1 de segell electrònic de nivell alt

La distribució de les dades d'activació per als certificats de dispositiu CDS, CDSCD, CDS-1 Seu electrònica de nivell mig i CDA-1 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-AL 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-AL 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-AL, 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-AL està identificat i reconegut abans d'utilitzar aplicacions crítiques relacionades amb el cicle de vida del certificat.
- El personal de l'EC-AL 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-AL (per exemple, certificats o informació d'estat de revocació) conta amb un control d'accésos 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 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-AL garanteix que les seves funcions de gestió de les operacions dels mòduls criptogràfics són suficientment segures i, en particular, ha d'assegurar que existeixen instruccions per:

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

L'EC-AL 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 planifiquen procediments per garantir suficient disponibilitat electrònica i d'emmagatzematge per als actius informatius.

6.6.3. Avaluació del nivell de seguretat del cicle de vida

Sense estipulació addicional.

6.7. Controls de seguretat de xarxa

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

7.2. Perfil de la llista de revocació de certificats

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

8. Auditoria de conformitat

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

8.1. Freqüència de l'auditoria de conformitat

L'EC-AL 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

CATCert pot encarregar-se de realitzar l'auditoria de conformitat.

No obstant això l'EC-AL 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-AL auditada. En cas d'auditoria interna, l'EC-AL 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 rebut l'informe de l'auditoria de compliment ja realitzada, l'EC-AL discuteix, amb l'entitat que ha executat l'auditoria i amb CATCert, les deficiències trobades i desenvolupa i executa un pla correctiu que soluciona les esmentades deficiències.

Si l'EC-AL 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-AL, de la forma com es descriu a la secció 4.9.

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

8.6. Tractament dels informes d'auditoria

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

9. Requisits comercials i legals

9.1. Tarifes

9.1.1 Tarifa d'emissió o renovació de certificats

CATCert estableix les tarifes que aplica l'EC-AL, 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

CATCert no practicarà 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.

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

9.2.2. Altres actius

Sense estipulació addicional.

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

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

9.3. Confidencialitat

9.3.1. Informacions confidencials

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

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

-
- b. Registres de transaccions, incloent els registres complets i els registres d'auditoria de les transaccions.
 - c. Registres d'auditoria interna i externa, creats i/o mantinguts per l'EC-AL i els seus auditors.
 - d. Plans de continuïtat de negoci i d'emergència.
 - e. Política i procediments de seguretat
 - f. Documentació d'operacions i restants plans d'operació, com ara arxiu, monitoratge i altres d'anàlegs.
 - g. Tota altra informació identificada com "Confidencial"

9.3.2. Informacions no confidencials

Les següents informacions no tenen caràcter confidencial:

- a. La política de certificació de l'EC-AL
- b. Aquesta Declaració de Pràctiques de Certificació de l'EC-AL
- c. Tota altra informació identificada com a "Pública"

9.3.3. Responsabilitat per la protecció d'informació confidencial

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

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

9.4. Protecció de dades personals

9.4.1. 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:

- Àmbit d'aplicació del document de seguretat amb especificació detallada dels recursos protegits (article 88 del RD 1720/2007) - secció 6.1.
- Mesures, normes, procediments, regles i estàndards que garanteixin el nivell de seguretat exigít pel RD 1720/2007 - secció 6.1, i, en general, tots els controls tècnics de les seccions 5 i 6 de la Política General de Certificació de CATCert.
- Funcions i obligacions del personal (article 89 del RD 1720/2007) - secció 5.3.
- Registre d'incidències (article 90 del RD 1720/2007), procediment de notificació, gestió i resposta davant les incidències – secció 9.4.5
- Control d'accés (article 91 del RD 1720/2007) – seccions 5 i 6.
- Gestió de suports (article 92 del RD 1720/2007) – secció 5.
- Identificació i autenticació (article 93 del RD 1720/2007) – secció 5.2.
- 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 qualsevol 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, 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 dona 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-AL concedeix llicència no exclusiva per reproduir, distribuir, verificar i utilitzar els certificats, sense cap cost, en relació amb firmes digitals i/o sistemes de xifrat dins de l'àmbit d'aplicació d'aquest document, d'acord amb el corresponent instrument vinculant entre l'EC-AL i la part que reproduceix i/o distribueix el certificat.

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

Addicionalment, els certificats emesos per l'EC-AL 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 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-AL 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 i altres compromisos

9.6.1.1.1. Obligacions de l'EC-AL

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

- L'EC-AL garanteix sota la seva plena responsabilitat, que compleix amb tots els requisits establerts en aquest document.
- L'EC-AL és l'única entitat responsable del compliment dels procediments descrits en aquest document, inclòs quan una part o la totalitat de les operacions siguin sub-contractades externament.
- L'EC-AL presta els seus serveis de certificació d'acord amb aquest document on es detallen almenys els continguts previstos en l'article 19 de la Llei 59/2003
- Abans de l'emissió i lliurament del certificat al subscriptor, l'EC-AL l'informa dels aspectes previstos en l'article 18. b) de la Llei 59/2003, i dels següents aspectes:
 - Indicació de la política aplicable, amb indicació que els certificats no s'expedeixen al públic i de la necessitat d'utilització de dispositiu segur de creació de signatura.
 - Forma en que es garanteix la responsabilitat patrimonial de l'EC-AL
 - L'EC-AL es declara d'acord amb la política de certificació, la certificació del prestador de serveis de certificació i la certificació dels productes de signatura electrònica utilitzats
- Aquest requisit es compleix mitjançant un "Text divulgatiu de la política de certificat" aplicable, que es transmet electrònicament, utilitzant un mitjà de comunicació durador en el temps, i en llenguatge comprensible.

-
- L'EC-AL 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-AL sense revocació de certificats vàlids.
 - Límits d'ús del certificat, incloent les establertes a la secció 4.5 d'aquest document.
 - Informació sobre com validar un certificat, incloent el requisit de comprovar l'estat del certificat, i les condicions en les quals es pot confiar raonablement en el certificat, que resulta aplicable quan el subscriptor actua com a verificador.
 - Limitacions de responsabilitat aplicables, incloent els usos pels quals l'EC-AL accepta o exclou la seva responsabilitat.
 - Procediments aplicables de resolució de disputes.
 - Llei aplicable i jurisdicció competent.
 - L'EC-AL identifica el subscriptor del certificat, 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-AL comprova per si mateixa o per mitjà d'una Entitat de Registre, la identitat i qualssevol altres circumstàncies personals dels sol·licitants dels certificats, d'acord amb l'establert en l'article 13 de la Llei 59/2003.
 - Quan el subscriptor del certificat de persona física (certificat de classe 1) és una persona jurídica, l'EC-AL comprova que el posseïdor de la clau es troba degudament autoritzat pel subscriptor.
 - L'EC-AL compleix la resta d'obligacions contingudes a l'article 12 de la Llei 59/2003

9.6.1.1.1. Informació per als certificats personals

L'EC-AL 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 certificant.

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

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

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

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

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

9.6.1.1.2. Obligacions de l'EC

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

- Determina la comunitat de subscriptors i verificadors de l'EC-AL.
- Aprova les polítiques de certificació i, si procedeix, les polítiques específiques de certificació.
- Aprova, si procedeix, aquest document la documentació contractual i reguladora dels serveis de certificació en la comunitat d'usuaris de l'EC-AL, d'acord amb el procediment previst en aquesta Declaració de Pràctiques de Certificació. i
- Informa puntualment l'EC-AL de totes les informacions relatives als canvis a realitzar, incidències en el servei, reclamacions, denúncies i inspeccions del servei.

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

9.6.1.2. Garanties ofertes a subscriptors i verificadors

L'EC-AL, 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-AL 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 certificant 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-AL, 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-AL 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-AL, amb els límits que s'estableixin.

9.6.2. Entitats de Registre

9.6.2.1. Obligacions i altres compromisos

9.6.2.1.1. Entitats de Registre Internes

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

- a. Actua exclusivament en relació amb persones vinculades a l'Entitat de Registre.
- b. Nomina 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 corresponent. Quan un operador deixa de tenir capacitat per actuar com el que és, sota el control i l'autoritat de l'Entitat de Registre, aquesta Entitat sol·licita de forma immediata a l'EC-AL la revocació del certificat d'operador corresponent.
- c. Valida i aprova les sol·licituds de certificats i tot seguit, genera les targetes per als posseïdors de claus, d'acord amb els procediments i instruments tècnics establerts per l'EC-AL, d'acord amb aquest document i la documentació d'operacions de l'EC-AL.
- d. Si l'Entitat de Registre Interna no disposa d'informació actualitzada del posseïdor de claus, comprova la identitat personalment o d'acord amb l'establert a l'article 13.4 de la Llei 59/2003, registra un justificant acreditatiu del nom complet, lloc i data de naixement, DNI i/o qualsevol altra informació que pugui ser utilitzada per diferenciar una persona respecte d'una altra en l'àmbit de l'Entitat de Registre Interna.
- e. Verifica, quan sigui necessari, qualsevol atribut específic del posseïdor de claus, i registrar un justificant acreditatiu de la informació.

- f. 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-AL, d'acord amb aquest document, i la documentació d'operacions de l'EC-AL.
- g. Emmagatzema els registres, ja sigui en paper, ja siguin de forma electrònica, amb les adequades mesures de seguretat, autenticitat, integritat i conservació, relatius a la informació continguda al certificat, durant un període de 15 anys. Aquests registres estan a disposició de l'EC-AL.
- h. Aporta la justificació documental necessària per al registre d'usuaris i per la posterior emissió de certificats per part de l'EC-AL o l'Entitat de Registre Col·laboradora.
- 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.

9.6.2.1.2. Entitat de Registre Col·laboradora

L'Entitat de Registre Col·laboradora queda obligada a registrar les dades del certificat i la seva aprovació en cas de ser correctes, així com al registre de les dades d'aquest certificat, per la qual cosa realitzarà les comprovacions que consideri necessàries sobre la identitat i la resta de dades personals i complementàries dels subscriptors, i si fos necessari, dels posseïdors de claus.

Aquestes comprovacions inclouen la justificació documental aportada pel sol·licitant certificador, i, si l'Entitat de Registre Col·laboradora ho considera necessari, qualsevol altre document i informació rellevant, facilitats pel subscriptor, pel posseïdor de claus o per terceres persones.

Si l'Entitat de Registre Col·laboradora detecta errors en les dades que estan incloses als certificats, o als documents que justifiquen aquestes dades, està obligada a realitzar els canvis que consideri necessaris abans de l'emissió del certificat, o a la paralització del procés d'emissió i a gestionar amb el subscriptor la incidència corresponent.

En el cas que l'Entitat de Registre Col·laboradora corregeixi les dades sense gestió prèvia de la incidència corresponent amb el subscriptor, queda obligada a notificar les dades que finalment se certifiquin al subscriptor en el moment del lliurament.

L'Entitat de Registre Col·laboradora es reserva el dret a no aprovar la sol·licitud d'emissió del certificat, quan la justificació documental aportada pel sol·licitant sigui insuficient per a la correcta identificació i/o autenticació del subscriptor, i si fos necessari, del posseïdor de claus.

9.6.2.2. Garanties ofertes a subscriptors i verificadors

9.6.2.2.1. Garantia de CATCert pels serveis de certificació digital

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

CATCert únicament garanteix que:

- a) Els certificats CPISR contenen tota la informació exigida per la Llei 59/2003, de 19 de desembre.
- b) CATCert no ha originat ni ha introduït declaracions falses o errònies en la informació de cap certificat, ni ha deixat d'incloure informació necessària aportada pel

subscriptor i validada per CATCert o per l'entitat de registre, en el moment de l'emissió del certificat.

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

d) CATCert queda vinculada pels procediments operatius, de seguretat i d'arxiu descrits en aquest document i a les seves Condicions Generals.

9.6.2.2.2. 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.

9.6.3. Subscriptors

9.6.3.1. Obligacions i altres compromisos

9.6.3.1.1. Informacions per a tots els tipus de certificats

L'EC-AL obliga el/la subscriptor a:

- a. Facilitar a l'EC-AL informació completa i adequada, en especial pel que respecta al procediment de registre.
- b. Manifestar el seu consentiment previ a l'emissió i entrega 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 firma electrònica.
- d. Utilitzar el certificat d'acord amb l'establert a la secció 1.4
- e. Notificar a l'EC-AL, sense endarreriments injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu segur de creació de firma.
- f. Notificar l'EC-AL i qualsevol persona que el subscriptor cregui que pugui confiar en el certificat, sense endarreriments injustificables:
 - 1) La pèrdua, el robatori o el compromís potencial de la seva clau privada.
 - 2) La pèrdua de control sobre la seva clau privada, a causa del compromís de les dades d'activació (per exemple, el codi PIN del dispositiu segur de creació de firma) o per qualsevol altra causa.
 - 3) 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 monitoritzar, 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.

9.6.3.1.2. Informacions específiques per als certificats de signatura electrònica reconeguda

L'EC-AL obliga el subscriptor a:

- a. Utilitzar el parell de claus exclusivament per a firmes electròniques i conforme a qualsevol altres limitacions que li siguin notificades.
- b. Reconèixer que aquestes firmes electròniques són firmes electròniques equivalents a firmes manuscrites, d'acord amb l'article 3.4 de la Llei 59/2003, de 19 de desembre.
- c. Ser especialment diligent en la custòdia de la seva clau privada i del seu dispositiu segur de creació de signatura, a fi d'evitar usos no autoritzats
- d. Notificar a l'EC-AL, sense retards 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 genera les seves pròpies claus, per tant, s'obliga a:
 1. Generar les seves claus de subscriptor utilitzant un algorisme reconegut com a acceptable per a la signatura electrònica reconeguda.
 2. Crear les claus dins del dispositiu segur de creació de signatura.
 3. Utilitzar longituds i algorismes de clau reconeguts com a acceptables per a la signatura electrònica reconeguda.

9.6.3.2. Garanties ofertes pel subscriptor

L'EC-AL obliga al subscriptor, mitjançant el corresponent instrument jurídic garantir:

- a. Que totes les manifestacions realitzades a la sol·licitud són correctes.
- b. Que totes les informacions subministrades pel subscriptor que es trobi contingudes al certificat són correctes.
- c. Que el certificat s'utilitza exclusivament per a usos legals i autoritzats, d'acord amb aquest document.
- d. Que 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. Que el subscriptor 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. Que cap persona no autoritzada no ha tingut mai accés a la clau privada del subscriptor.

9.6.3.3. Protecció de la clau privada

L'EC-AL 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.

9.6.4. Verificadors

9.6.4.1. Obligacions i altres compromisos

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

- a. Assessorar-se sobre el fet que el certificat és apropiat per a l'ús que es pretén.
- b. Verificar la validesa, suspensió o revocació dels certificats emesos, per a la qual cosa utilitza informació sobre l'estat dels certificats.
- c. Verificar tots els certificats de la jerarquia de certificats, abans de confiar en la signatura digital o en algun dels certificats de la jerarquia.
- d. Tenir present qualsevol limitació en l'ús del certificat, amb independència que es trobi al mateix certificat o al contracte de verificador.
- e. Tenir present qualsevol precaució establerta en un contracte o en un altre instrument, amb independència de la seva naturalesa jurídica.
- f. No monitoritzar, manipular o realitzar actes d'enginyeria inversa sobre la implantació tècnica de la jerarquia pública de certificació de Catalunya, sense permís previ per escrit.
- g. No comprometre intencionadament la seguretat de la jerarquia pública de certificació de Catalunya.
- h. Reconèixer que les firmes electròniques produïdes per certificats CPISR i CEISR són firmes electròniques equivalents a firmes escrites, d'acord amb l'art. 3.4 de la Llei 59/2003, de 19 de desembre.

9.6.4.2. Garanties ofertes pel verificador

L'EC-AL 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 en 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.

9.6.5. Altres participants

9.6.5.1. Obligacions i garanties del directori

L'EC-AL 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 Registre s'estableixen detalladament en aquest document, així com en la documentació jurídica auxiliar, especialment la lliurada a subscriptors, posseïdors de claus i verificadors.

9.6.5.2. Garanties ofertes pel directori

L'EC-AL té la responsabilitat civil sobre el directori de certificació, quan sigui operat per una tercera entitat.

9.7. Renúncies de garanties

9.7.1. Rebuig de garanties de la EC-AL

L'EC-AL 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 la EC-AL

L'EC-AL 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-AL pot limitar la seva responsabilitat mitjançant la inclusió de límits d'ús del certificat, i límits de valor de les transaccions per a les quals es pot utilitzar el certificat.

9.8.2. Cas fortuït i força major

L'EC-AL 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-AL 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-AL 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-AL 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-AL vetlla perquè, almenys els requisits continguts a les seccions Obligacions, 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-AL amb subscriptors i verificadors.

CATCert determinarà un Pla de Continuïtat de Negoci. Aquest Pla de Continuïtat 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-AL 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 es tindrà en compte:

- La modificació haurà d'estar justificada des del punt de vista tècnic, legal o comercial.
- La modificació proposada per l'EC-AL no podrà anar en contra de la política de certificació establerta per CATCert.
- S'establirà un control de modificacions, per garantir, en tot cas, que les especificacions resultants compleixen els requisits que s'intentaven complir i que van donar peu al canvi.
- S'establiran les implicacions que el canvi d'especificacions té sobre l'usuari, i es preveurà 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-AL 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-AL.

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

9.13.2. Jurisdicció competent

L'EC-AL 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-AL tingui la consideració d'Administració Pública es té en compte la legislació administrativa que resulti aplicable.

9.14. Llei aplicable

L'EC-AL 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-AL continuï establerta a 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-AL manifesta el compliment de la Llei 59/2003, en aquest document.

9.16. Clàusules diverses

9.16.1. Acord íntegre

L'EC-AL 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 es pot subrogar 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-AL.

9.16.3. Divisibilitat

L'EC-AL 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 la clàusules indicades.

9.16.4. Aplicacions

Sense estipulació addicional.

9.16.5. Altres clàusules

Sense estipulació addicional.

ANNEX I

Control documental

Projecte:	Informe modificació del document DPC EC-AL
Entitat de destí:	Agència Catalana de Certificació
Codi de referència:	Revisió 1r semestre 2010
Versió:	Canvis de la v3.5 REF a la 3.6 en català i en castellà
Data de l'edició:	03/12/2010

Control de versions DPC EC-AL 2n semestre 2010

Versió	Parts que canvien	Descripció del canvi	Autor del canvi	Data del canvi
3.4	Tot el text	Correccions de caràcter ortogràfic i tipogràfic	Oficina de Polítiques	13/04/2010
3.5 REF	Apartat 4	Inclusió del procés telemàtic	Oficina de Polítiques	20/04/2010
3.5 REF	Tot el text	Repàs i correccions ortogràfiques	Oficina de Polítiques	17/09/2010
3.6	Apartats 4.9.1 i 5.5	Adaptació CAB/Forum Extended Validation	Oficina de Polítiques	03/12/2010