




**Agència Catalana
de Certificació**

Declaració de Pràctiques de Certificació
Entitat de Certificació PARLAMENT

(EC-PARLAMENT)

Referència: D1111_E0650_N-DPC EC-GENCAT
Versió: 1.6
Data: 31/06/2011

Control documental

Estat formal	Elaborat per: Carlos Alonso – Núria Mombiola (Àrea d'Assessorament)	Aprovat per: Marta Cruellas
Data de creació	17/07/2006	
Control de versions	Data:	
	Descripció:	Expliqueu breument quins són els darrers canvis introduïts respecte la versió anterior (p.e. "Creació de document", "Modificació dels preus", "Adaptació dels apartats 1.2 i 2.5 a la Llei 59/2003", etc.)
Nivell accés informació	pública	
Títol	Declració de Pràctiques de Certificació EC-PARLAMENT v1r6 cat	
Fitxer	D1111 E0650 N-DPC EC-GENCAT v1r6 cat.pdf	
Control de còpies	Només les còpies disponibles a https://www.catcert.cat/ garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.	
Drets d'autor	 <p>Aquesta obra està subjecta a una llicència Reconeixement-No comercial-Sense obres derivades 2.5 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.</p>	

Índex

Índex	3
1. Introducció.....	11
1.1 PRESENTACIÓ	11
1.1.1 Tipus i classes de certificats	11
1.1.2 Relació entre la Declaració de Pràctiques de Certificació (DPC) i altres documents.....	17
1.2 NOM DEL DOCUMENT I IDENTIFICACIÓ.....	17
1.2.1 Identificació d'aquest document.....	17
1.2.2 Identificació de polítiques de certificació cobertes per aquesta DPC	17
1.3 COMUNITAT D'USUARIS DE CERTIFICATS.....	19
1.3.1 Prestadors de serveis de certificació	20
1.3.2 Entitat de Certificació Arrel	20
1.3.3 EC-PARLAMENT	21
1.3.4 Entitats de Registre.....	21
1.3.5 Usuaris finals	22
1.4 ÚS DELS CERTIFICATS.....	23
1.4.1 Usos típics dels certificats.....	24
1.4.2 Aplicacions prohibides	32
1.5 ADMINISTRACIÓ DE LA DECLARACIÓ DE PRÀCTIQUES.....	35
1.5.1 Organització que administra l'especificació	35
1.5.2 Dades de contacte de l'organització	35
1.5.3 Persona que determina la conformitat de la Declaració de Pràctiques de Certificació (DPC) amb la política	36
1.5.4 Procediment d'aprovació	36
2. Publicació d'informació i directori de certificats	37
2.1 DIRECTORI DE CERTIFICATS	37
2.2 PUBLICACIÓ D'INFORMACIÓ DE L'EC-PARLAMENT	37
2.3 FREQUÈNCIA DE PUBLICACIÓ	37
2.4 CONTROL D'ACCÉS	37
3. Identificació i autenticació	39
3.1 GESTIÓ DE NOMS	39
3.1.1 Tipus de noms	39
3.1.2 Significat dels noms.....	39
3.1.3 Utilització d'anònims i pseudònims	39
3.1.4 Interpretació de formats de noms	39

3.1.5.	Unicitat dels noms.....	39
3.1.6.	Resolució de conflictes relatius a noms.....	40
3.2.	VALIDACIÓ INICIAL DE LA IDENTITAT.....	42
3.2.1.	Prova de possessió de clau privada.....	42
3.2.2.	Autenticació de la identitat d'una Organització.....	42
3.2.3.	Autenticació de la identitat d'una persona física.....	44
3.2.4.	Informació no verificada.....	45
3.3.	IDENTIFICACIÓ I AUTENTICACIÓ DE SOL·LICITUDS DE RENOVACIÓ.....	45
3.3.1.	Validació per a la renovació rutinària de certificats.....	45
3.3.2.	Validació per a la renovació de certificats després de la revocació.....	45
4.	Característiques d'operació del cicle de vida dels certificats	46
4.1.	SOL·LICITUD D'EMISSIÓ DE CERTIFICAT.....	46
4.1.1.	Legitimació per a sol·licitar l'emissió.....	46
4.1.2.	Procediment d'alta: Responsabilitats.....	46
4.2.	PROCESSAMENT DE LA SOL·LICITUD DE CERTIFICACIÓ.....	47
4.2.1.	Requisits per a tots tipus de certificats	47
4.2.2.	Requisits específics per al CEIXSA	48
4.2.3.	Requisits addicionals per al CDS-1, CDS-1 EV, el CDSCD-1 i el CDS-1 Seu electrònica EV	48
4.2.4.	Requisits específics per al CIPISR	48
4.2.5.	Altres certificats.....	49
4.3.	EMISSIÓ DE CERTIFICAT.....	49
4.3.1.	Accions de l'EC-PARLAMENT durant el procés d'emissió.....	49
4.3.2.	Notificació de l'emissió al subscriptor	50
4.4.	ACEPTACIÓ DEL CERTIFICAT	50
4.4.1.	Responsabilitats de l'EC-PARLAMENT	50
4.4.2.	Conducta que constitueix acceptació del certificat	52
4.4.3.	Publicació del certificat	52
4.4.4.	Notificació de l'emissió a tercers.....	52
4.5.	ÚS DEL PARELL DE CLAUS I DEL CERTIFICAT	52
4.5.1.	Ús del parell de claus pels posseïdors de claus i ús del certificat pels subscriptors.....	52
4.5.2.	Ús pel tercer que confia en certificats.....	54
4.6.	RENOVACIÓ DE CERTIFICATS SENSE RENOVACIÓ DE CLAUS	54
4.7.	RENOVACIÓ DE CERTIFICATS AMB RENOVACIÓ DE CLAUS.....	54
4.8.	MODIFICACIÓ DE CERTIFICATS.....	55

4.9.	REVOCACIÓ I SUSPENSIÓ DE CERTIFICATS.....	55
4.9.1.	Causes de revocació de certificats	55
4.9.2.	Legitimació per a sol·licitar la revocació	57
4.9.3.	Procediments de sol·licitud de revocació.....	57
4.9.4.	Període temporal de sol·licitud de revocació	57
4.9.5.	Període màxim de processament de la sol·licitud de revocació	58
4.9.6.	Obligació de consulta d'informació de revocació de certificats.....	58
4.9.7.	Freqüència d'emissió de llistes de revocació de certificats (LRCs)	58
4.9.8.	Període màxim de publicació de LRCs.....	58
4.9.9.	Disponibilitat de serveis de comprovació d'estat de certificats	58
4.9.10.	Obligació de consulta dels serveis de comprovació d'estat de certificats ...	58
4.9.11.	Altres formes d'informació de revocació de certificats	59
4.9.12.	Requisits especials en cas de compromís de la clau privada	59
4.9.13.	Causes de suspensió de certificats.....	59
4.9.14.	Legimitat per sol·licitar la suspensió.....	60
4.9.15.	Procediments de sol·licitud de suspensió	60
4.9.16.	Període màxim de suspensió	61
4.9.17.	Habilitació d'un certificat suspès	61
4.10.	SERVEIS DE COMPROVACIÓ D'ESTAT DE CERTIFICATS.....	61
4.10.1.	Característiques d'operació dels serveis.....	61
4.10.2.	Disponibilitat dels serveis	61
4.10.3.	Altres funcions dels serveis.....	61
4.11.	ACABAMENT DE LA SUBSCRIPCIÓ	61
4.12.	DIPÒSIT I RECUPERACIÓ DE CLAUS.....	61
4.12.1	Política i pràctiques de dipòsit i recuperació de claus.....	61
4.12.2.	Política i pràctiques d'encapsulament i recuperació de claus de sessió	62
5.	Controls de seguretat física, de gestió i d'operacions.....	63
5.1.	CONTROLS DE SEGURETAT FÍSICA	63
5.1.1.	Localització i construcció de les instal·lacions.....	64
5.1.2.	Accés físic.....	64
5.1.3.	Electricitat i aire condicionat	64
5.1.4.	Exposició a l'aigua	65
5.1.5.	Advertència i protecció d'incendis.....	65
5.1.6.	Emmagatzematge de suports	65
5.1.7.	Tractament de residus	65

5.1.8.	Còpia de seguretat fora de les instal·lacions	65
5.2.	CONTROLS DE PROCEDIMENTS	66
5.2.1.	Funcions fiables	66
5.2.2.	Nombre de persones per tasca.....	66
5.2.3.	Identificació i autenticació per a cada funció	66
5.2.4.	Rols que requereixen separació de tasques.....	66
5.3.	CONTROLS DE PERSONAL	67
5.3.1.	Requisits d'historial, qualificacions, experiència i autorització.....	68
5.3.2.	Requisits de formació	68
5.3.3.	Requisits i freqüència d'actualització formativa	69
5.3.4.	Seqüència i freqüència de rotació laboral.....	69
5.3.5.	Sancions per accions no autoritzades	69
5.3.6.	Requisits de contractació de professionals.....	69
5.3.7.	Subministrament de documentació al personal	70
5.4.	PROCEDIMENTS D'AUDITORIA DE SEGURETAT	70
5.4.1.	Tipus d'esdeveniments registrats	70
5.4.2.	Freqüència de tractament de registres d'auditoria.....	71
5.4.3.	Període de conservació de registres d'auditoria.....	71
5.4.4.	Protecció dels registres d'auditoria	71
5.4.5.	Procediments de còpies de seguretat.....	71
5.4.6.	Localització del sistema d'acumulació de registres d'auditoria.....	72
5.4.7.	Notificació de l'esdeveniment d'auditoria al causant de l'esdeveniment	72
5.4.8.	Anàlisi de vulnerabilitats.....	72
5.5.	ARXIU D'INFORMACIONS	72
5.5.1.	Tipus d'esdeveniments registrats	72
5.5.2.	Període de conservació de registres	73
5.5.3.	Protecció de l'arxiu.....	73
5.5.4.	Procediments de còpia de suport	73
5.5.5.	Requisits de segellat de cautela de data i hora	73
5.5.6.	Localització del sistema d'arxiu	73
5.5.7.	Procediments d'obtenció i verificació d'informació d'arxiu	74
5.6.	RENOVACIÓ DE CLAUS	74
5.7.	COMPROMÍS DE CLAUS I RECUPERACIÓ DE DESASTRES	74
5.7.1.	Procediment de gestió d'incidències i compromisos	74
5.7.2.	Corrupció de recursos, aplicacions o dades	74

5.7.3.	Compromís de la clau privada de l'Entitat	74
5.7.4.	Desastre sobre les instal·lacions	74
5.8.	FINALITZACIÓ DEL SERVEI	75
5.8.1.	EC-PARLAMENT	75
5.8.2.	Entitat de Registre	75
6.	Controls de seguretat tècnica.....	76
6.1.	GENERACIÓ I INSTAL·LACIÓ DEL PARELL DE CLAUS	76
6.1.1.	Generació del parell de claus	76
6.1.2.	Tramesa de la clau privada al subscriptor	77
6.1.3.	Tramesa de la clau pública a l'emissor del certificat.....	77
6.1.4.	Distribució de la clau pública del Prestador de Serveis de Certificació	77
6.1.5.	Mides de claus	78
6.1.6.	Generació de paràmetres de clau pública	78
6.1.7.	Comprovació de la qualitat dels paràmetres de clau pública.....	78
6.1.8.	Generació de claus en aplicacions informàtiques o en béns d'equip	78
6.1.9.	Propòsits d'ús de claus	78
6.2.	PROTECCIÓ DE LA CLAU PRIVADA	79
6.2.1.	Mòduls de protecció de la clau privada.....	79
6.2.2.	Control per part de més d'una persona (n de m) sobre la clau privada.....	79
6.2.3.	Dipòsit de la clau privada.....	79
6.2.4.	Còpia de seguretat de la clau privada	80
6.2.5.	Arxiu de la clau privada.....	80
6.2.6.	Introducció de la clau privada en el mòdul criptogràfic	80
6.2.7.	Emmagatzematge de la clau privada en el mòdul criptogràfic	80
6.2.8.	Mètode d'activació de la clau privada	80
6.2.9.	Mètode de desactivació de la clau privada	80
6.2.10.	Mètode de destrucció de la clau privada.....	80
6.2.11.	Classificació dels mòduls criptogràfics.....	81
6.3.	ALTRES ASPECTES DE GESTIÓ DEL PARELL DE CLAUS.....	81
6.3.1.	Arxiu de la clau pública	81
6.3.2.	Períodes d'utilització de les claus pública i privada	81
6.4.	DADES D'ACTIVACIÓ	81
6.4.1.	Generació i instal·lació de les dades d'activació	81
6.4.2.	Protecció de les dades d'activació.....	81
6.4.3.	Altres aspectes de les dades d'activació	82

6.5.	CONTROLS DE SEGURETAT INFORMÀTICA.....	82
6.5.1.	Requisits tècnics específics de seguretat informàtica	82
6.5.2.	Avaluació del nivell de seguretat informàtica.....	83
6.6.	CONTROLS TÈCNICS DEL CICLE DE VIDA	83
6.6.1.	Controls de desenvolupament de sistemes	83
6.6.2.	Controls de gestió de seguretat	83
6.6.3.	Avaluació del nivell de seguretat del cicle de vida.....	83
6.7.	CONTROLS DE SEGURETAT DE XARXA.....	83
6.8.	SEGELL DE TEMPS	84
7.	Perfils de certificats i llistes de certificats revocats	85
7.1.	PERFIL DE CERTIFICAT	85
7.2.	PERFIL DE LA LLISTA DE REVOCACIÓ DE CERTIFICATS.....	85
8.	Auditoria de conformitat.....	86
8.1.	FREQÜÈNCIA DE L'AUDITORIA DE CONFORMITAT	86
8.2.	IDENTIFICACIÓ I QUALIFICACIÓ DE L'AUDITOR.....	86
8.3.	RELACIÓ DE L'AUDITOR AMB L'ENTITAT AUDITADA.....	86
8.4.	RELACIÓ D'ELEMENTS OBJECTE D'AUDITORIA	86
8.5.	ACCIONS A EMPRENDRE COM A RESULTAT D'UNA FALTA DE CONFORMITAT	86
8.6.	TRACTAMENT DELS INFORMES D'AUDITORIA	87
9.	Requisits comercials i legals	88
9.1.	TARIFES	88
9.1.1.	Tarifa d'emissió o renovació de certificats	88
9.1.2.	Tarifa d'accés a certificats	88
9.1.3.	Tarifa d'accés a informació d'estat de certificat	88
9.1.4.	Tarifes d'altres serveis	88
9.1.5.	Política de reintegrament.....	88
9.2.	CAPACITAT FINANCERA.....	88
9.2.1.	Assegurança de responsabilitat civil.....	88
9.2.2.	Altres actius	88
9.2.3.	Cobertura d'assegurament per a subscriptors i tercers que confien en certificats	88
9.3.	CONFIDENCIALITAT	88
9.3.1.	Informacions confidencials.....	88
9.3.2.	Informacions no confidencials.....	89
9.3.3.	Responsabilitat per la protecció d'informació confidencial	89
9.4.	PROTECCIÓ DE DADES PERSONALS	89
9.4.1.	Política de Protecció de Dades Personals.....	89
9.4.2.	Dades de caràcter personal no disponibles a tercers.....	90

9.4.3.	Dades de caràcter personal disponibles a tercers	91
9.4.4.	Responsabilitat corresponent a la protecció de les dades personals	92
9.4.5.	Gestió d'incidències relacionades amb les dades de caràcter personal	92
9.4.6.	Prestació del consentiment per al tractament de les dades personals	93
9.4.7.	Comunicació de dades personals	93
9.5.	DRETS DE PROPIETAT INTEL·LECTUAL	93
9.5.1.	Propietat dels certificats i informació de revocació	93
9.5.2.	Propietat de la Política de Certificació i Declaració de Pràctiques de Certificació	94
9.5.3.	Propietat de la informació relativa a noms	94
9.5.4.	Propietat de claus	94
9.6.	OBLIGACIONS I RESPONSABILITAT CIVIL	94
9.6.1.	EC-PARLAMENT	94
9.6.2.	Obligaciones y otros compromisos de las Entidades de Registro	97
9.6.3.	Subscriptors	98
9.6.4.	Verificadors	100
9.6.5.	Altres participants	101
9.7.	RENÚNCIES DE GARANTIES	101
9.7.1.	Rebuig de garanties de l'EC-PARLAMENT	101
9.8.	LIMITACIONS DE RESPONSABILITAT	102
9.8.1.	Limitacions de responsabilitat de l'EC-PARLAMENT	102
9.8.2.	Cas fortuït i força major	102
9.9.	INDEMNITZACIONS	102
9.9.1.	Clàusula d'indemnitat de subscriptor	102
9.9.2.	Clàusula d'indemnitat de verificador	102
9.10.	TERMINI I FINALITZACIÓ	102
9.10.1.	Termini	102
9.10.2.	Finalització	102
9.10.3.	Supervivència	102
9.11.	NOTIFICACIONS	103
9.12.	MODIFICACIONS	103
9.12.1.	Procediment per a les modificacions	103
9.12.2.	Termini i mecanismes per a notificacions	103
9.12.3.	Circumstàncies en les que un OID ha de ser canviat	103
9.13.	RESOLUCIÓ DE CONFLICTES	104
9.13.1.	Resolució extrajudicial de conflictes	104

9.13.2.	Jurisdicció competent.....	104
9.14.	LLEI APLICABLE.....	104
9.15.	CONFORMITAT AMB LA LLEI APLICABLE.....	104
9.16.	CLÀUSULES DIVERSES	104
9.16.1.	Acord íntegre.....	104
9.16.2.	Subrogació	105
9.16.3.	Divisibilitat	105
9.16.4.	Aplicacions	105
9.16.5.	Altres clàusules	105
2.	106

1. Introducció

1.1 Presentació

El Parlament de Catalunya i el Consorci de l'Administració Oberta Electrònica de Catalunya varen signar en data 18 de juny de 2004, l'Acord Institucional d'impulsar l'ús de les tecnologies de la informació i de la comunicació, i per a implantar nous serveis i instruments per a la tramitació telemàtica al Parlament de Catalunya.

Entre els pactes adoptats en aquest Acord Institucional, es va acordar la creació de l'Entitat de certificació "Parlament de Catalunya" (EC-PARLAMENT), vinculada a la jerarquia d'entitats de certificació públiques de Catalunya, els serveis a desenvolupar de la qual varen quedar reflectits en el Conveni de col·laboració subscrit pel Parlament de Catalunya i l'Agència Catalana de Certificació, en data 18 de juny de 2004.

L'EC-PARLAMENT és una Entitat de Certificació Virtual, de la qual n'és titular el Parlament de Catalunya i operada per CATCert.

El Parlament de Catalunya, i tanmateix aquelles institucions dependents orgànicament d'aquest degudament autoritzades, actua com a Entitat de Registre, de manera que, com a subscriptor dels certificats, registra directament als seus posseïdors de claus, encarregant-se de la identificació, el registre, la validació de les sol·licituds i l'expedició dels certificats i les targetes.

Tanmateix, el Parlament de Catalunya, quan és necessari, sol·licita la suspensió, habilitació, revocació o renovació dels certificats que emet com a Entitat de Certificació.

1.1.1 Tipus i classes de certificats

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

Els certificats d'usuaris finals emesos per l'EC-PARLAMENT es divideixen en:

- Certificats d'infraestructura, caracteritzats pel fet que el posseïdor de la clau privada és un operador d'una infraestructura, i que s'utilitza per autoritzar operacions relacionades amb els serveis de certificació, com l'aprovació de sol·licituds de certificació.
- Certificats personals, caracteritzats pel fet que el posseïdor de la clau privada és una persona física que actua en el seu propi nom i representació (essent, en aquest cas subscriptor o titular del certificat), o en representació i per compte d'una persona jurídica (que serà el subscriptor o titular del certificat)
- Certificats de dispositiu, caracteritzats pel fet que el posseïdor de la clau privada és un dispositiu informàtic que realitza les operacions de signatura i desxifrat de manera automàtica, sota la responsabilitat d'una persona física o jurídica (denominada subscriptor o titular del certificat).
- Certificats d'entitat, caracteritzats pel fet que el subscriptor del certificat i, d'acord amb la llei, el signant, és una persona física que actua per mitjà d'un posseïdor de claus (també anomenat per a aquests certificats com a "responsable de custòdia").

Els certificats d'usuari s'emetran en la modalitat de classe 1 i de classe 2.

Els certificats de classe 1 són certificats d'organització del sector públic de Catalunya (corporatius), caracteritzats pel fet que la persona física posseïdora de la clau privada té una vinculació amb el subscriptor o titular del certificat, què és una persona jurídica .

Els certificats de classe 2 són la resta de certificats no inclosos en la definició anterior, emesos en concurrència amb el lliure mercat i, habitualment, en règim d'actuació subsidiària, quan no existeixin prestadors que ofereixin el servei o el nombre d'aquests esdevingui insuficient per a garantir la seva distribució efectiva als usuaris finals. El registre de les dades per a l'emissió dels certificats de classe 2 es realitza per les Entitats de Registre. Aquests certificats de classe 2 es subdivideixen, alhora, en individuals o col·lectius en funció de si s'expedeixen a una persona física que actua en nom propi, o a una organització que actua per mitjà d'una persona física, identificada en el certificat.

1.1.1.1 Certificats d'infraestructura

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

- 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-PARLAMENT emet els següents tipus de certificats personals:

- Certificats personals d'identitat i signatura electrònica reconeguda de classe 1 amb càrrec (CIPISR-1 amb Càrrec), que identifiquen a la persona que els posseeix, la seva organització subscriptora, el seu càrrec dins la mateixa, i que serveixen per a signar missatges amb dispositiu segur de creació de signatura, i tanmateix missatges d'autenticació i d'accés segur a sistemes informàtics.

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

El certificat 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. 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. 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 manuscrita, sinó només la identificació del posseïdor de claus, en nom de la Institució.

El certificat personal d'identitat i signatura electrònica reconeguda de classe 2 amb càrrec (CPISR-2 Càrrec) és un certificat reconegut d'acord amb allò que estableix 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 acomplint amb les obligacions dels articles 12, 13, 18 i 20 de la citada Llei. 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 a allò que disposa la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. Garanteix la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permet la generació de la "signatura electrònica reconeguda", és a dir, la signatura electrònica avançada que es basa en un certificat reconegut i que ha estat generada utilitzant un dispositiu segur, per la qual cosa, de conformitat amb allò que estableix l'article 3 de la Llei 59/2003, de 19 de desembre, s'equipara amb la signatura escrita per efecte legal, sense necessitat de compliment de cap altre requisit addicional. 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.

El certificat personal de xifrat de classe 1 amb càrrec (CPX-1 amb 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. Funcionen amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i que compleixen allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. Garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten xifrar documents i rebre missatges de dades confidencials, en qualsevol format.

El certificat personal de xifrat de classe 2 amb càrrec (CPX-2 càrrec), és un certificat reconegut de conformitat amb el que s'estableix a l'article 6 i 11.1, amb el contingut prescrit per l'article 11.2 i emès complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica. Funcionen amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i que compleixen allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. Garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten xifrar documents i rebre missatges de dades confidencials, en qualsevol format.

El certificat personal d'identificació, xifrat i signatura avançada amb càrrec d'empleat públic de classe 1 (CPIXSA-1 Càrrec EP) és un certificat reconegut de conformitat amb el que s'estableix a l'article 6 i 11.1, amb el contingut prescrit per l'article 11.2 i emès complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica. Garanteix la identitat del subscriptor i el posseïdor de la clau privada d'identificació i signatura, i permet la generació de la "signatura electrònica avançada".

1.1.1.3 Certificats d'entitat

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

- Certificat d'entitat d'identificació i signatura electrònica reconeguda de classe 1 (CEISR-1), d'acord amb allò que estableix 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 jurídic-públiques (col·lectivament denominades "entitats") signin documents amb dispositiu segur de creació de

signatura, missatges d'autenticació (confirmació de la identitat) i d'accés segur a sistemes informàtics.

- Certificat d'entitat de xifrat de classe 1 (CEX-1), d'acord amb allò que estableix 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 jurídic-públiques (col·lectivament denominades "entitats") puguin produir i rebre documents confidencials.
- Certificats d'entitat d'identificació, xifrat i signatura electrònica avançada (CEIXSA) d'acord amb l'establert en l'article 7 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, que permet que Institucions públiques i privades, corporacions de dret públic i persones jurídic-públiques (col·lectivament denominades "entitats") signin documents electrònicament, missatges d'autenticació (confirmació de la identitat) i d'accés segur a sistemes informàtics i puguin produir i rebre documents confidencials.

A més a més, en funció dels requisits tècnics i de les necessitats dels usuaris, és possible que aquests tipus de certificats puguin incorporar d'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-PARLAMENT emet els següents tipus de certificat de dispositiu:

- Certificat de dispositiu servidor segur de classe 1 (CDS-1), que és utilitzat per una aplicació informàtica, servidor SSL o TLS, per a identificar-se davant les aplicacions client que es connecten i per a protegir el secret de les comunicacions entre el client i el servidor.
- Certificat de dispositiu servidor segur de classe 1 Extended Validation (CDS-1 EV), que s'utilitza per una aplicació informàtica, servidor de SSL o de TLS, perquè s'identifiqui davant de les aplicacions client que es connecten i per protegir el secret de les comunicacions entre el client i el servidor, tot oferint la validació automàtica al navegador.
- Certificat de dispositiu d'aplicació digitalment assegurada de classe 1 (CDA-1), que és utilitzat per a aplicacions informàtiques que s'identifiquen digitalment, signen electrònicament *webservices* o d'altres protocols i que reben documents i missatges xifrats.
- Certificat de dispositiu software o de signatura d'aplicacions informàtiques de classe 1 (CDP-1), que s'utilitza per a signar electrònicament les aplicacions informàtiques o software a transmetre a través de xarxes (Internet...) D'aquesta manera, els usuaris finals poden signar elements com applets, scripts, executables, etc.
- Certificat de dispositiu segur de controlador de dominis de classe 1 (CDSCD-1), que és utilitzat 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 de seu electrònica nivell mig de classe 1 Extended Validation (CDS-1 SENM EV), que serveix per identificar i garantir una comunicació segura amb la seu electrònica d'un ens, entenent seu electrònica en els termes que la

descriu l'article 10 de la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics.

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

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

Aquest certificat 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, tot oferint la validació automàtica al navegador.

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

El certificat de nivell alt s'haurà d'emmagatzemar en un HSM (maquinari criptogràfic).

- Certificat de dispositiu de segell electrònic de Administració, òrgan o entitat de dret públic nivell mig de classe 1 (CDA-1 SENM), 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 SENA), serveix per a la identificació i l'autenticació de l'exercici de la competència en l'actuació administrativa

automatitzada, en els termes descrits en l'article 18 de la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics.

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

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

El certificat de segell electrònic de nivell alt es carregarà directament a la PSIS (Plataforma de serveis d'identificació i signatura), almenys mentre no es disposi del maquinari criptogràfic HSM necessari per al nivell de seguretat requerit.

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

1.1.2 Relació entre la Declaració de Pràctiques de Certificació (DPC) i altres documents

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

L'EC-PARLAMENT emet certificats dintre de la Jerarquia de l'Agència Catalana de Certificació. Per tant, disposa d'una Declaració de Pràctiques de Certificació (DPC) d'acord amb la Política General de Certificació de CATCert, que inclou els procediments que aplica l'EC-PARLAMENT a 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-PARLAMENT".

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

1.3.6.1.4.1.15096.1.2. 8

1.2.2 Identificació de polítiques de certificació cobertes per aquesta DPC

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

- **CIPISR** – Certificat d'infraestructura d'operador, emès per l'EC-PARLAMENT

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.15

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.16

- **CIC** – Certificat d'infraestructura d'Entitat de Certificació Vinculada, emès per l'EC-PARLAMENT

CIC-2. OID: 1.3.6.1.4.1.15096.1.3.1.12

- **CIDS-1** – Certificat de infraestructura de servidor segur, emès per l'EC-PARLAMENT

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.17

- **CIDA-1** – Certificat d'infraestructura d'aplicació, emès per l'EC-PARLAMENT

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.18

- **CIO-1** – Certificat d'infraestructura de servidor d'estat de certificats en línia, emès per l'EC-PARLAMENT

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.19

- **CIV-1** – Certificat d'infraestructura d'entitat de validació, emès per l'EC-PARLAMENT

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.20

- **CIT-1** - Certificat d'infraestructura d'entitat de segells de temps, emès per l'EC-PARLAMENT

Classe 1. 1.3.6.1.4.1.15096.1.3.1.111

- **CPISR-1 amb Càrrec** - Certificat personal d'identificació i signatura electrònica reconeguda amb Càrrec, emès per l'EC-PARLAMENT

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.2.2

- **CPISR-1 amb Càrrec i Ús** – Certificat personal d'identificació i signatura electrònica reconeguda amb Càrrec i Ús concret, emès per l'EC-PARLAMENT

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.3.4

- **CPISR-2 amb Càrrec** - Certificat personal d'identificació i signatura electrònica reconeguda amb Càrrec, emès per l'EC-PARLAMENT

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.82.3.2

- **CPX amb Càrrec** - Certificat personal de xifrat amb Càrrec, emès per l'EC-PARLAMENT

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.41 .1.2

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.42.3.2

- **CPIXSA-1 Càrrec EP** – Certificat personal d'identificació, xifrat i signatura electrònica avançada amb càrrec d'empleat públic, emès per l'EC-PARLAMENT

OID: 1.3.6.1.4.1.15096.1.3.1.85

- **CEISR-1** - Certificat d'entitat d'identificació i signatura electrònica reconeguda, emès per l'EC-PARLAMENT.

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.121.4

- **CEX-1** - Certificat d'entitat de xifrat, emès per l'EC-PARLAMENT.

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.131.4

- **CEIXSA-1** – Certificats d'entitat d'identificació, xifrat i signatura electrònica avançada emès per l'EC-PARLAMENT
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.161.4
- **CDS-1**- Certificat de dispositiu servidor segur, emès per l'EC-PARLAMENT
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51
- **CDS-1 EV**- Certificat de dispositiu servidor segur Extended Validation, emès per l'EC-PARLAMENT
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.4
- **CDSCD-1**- Certificat de dispositiu segur de controlador de domini, emès per l'EC-PARLAMENT.
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.1
- **CDA-1**- Certificat de dispositiu d'aplicació digitalment assegurada (CDA), emès per l'EC-PARLAMENT.
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.91
- **CDP-1**- Certificat de dispositiu software o de signatura d'aplicacions informàtiques, emès per l'EC-PARLAMENT.
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.71
- **CDS-1 Seu electrònica nivell mig EV** – Certificat de dispositiu servidor segur, seu electrònica nivell mig Extended Validation, emès per l'EC-PARLAMENT
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.2
- **CDS-1 Seu electrònica nivell alt EV** – Certificat de dispositiu servidor segur, seu electrònica nivell alt Extended Validation, emès per l'EC-PARLAMENT
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.3
- **CDA-1 segell electrònic nivell mig** - Certificat de dispositiu d'aplicació digitalment assegurada, segell electrònic nivell mig, emès per l'EC-PARLAMENT
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-PARLAMENT
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.91.2

1.3 Comunitat d'usuaris de certificats

La present DPC regula una comunitat d'usuaris que obtenen certificats per a diverses relacions administratives i privades, d'acord amb la Llei 59/2003, de 19 de desembre, de signatura electrònica i la normativa administrativa corresponent.

Els certificats de l'EC-PARLAMENT no són expedits al públic, sinó a:

- Parlamentaris,
- Personal d'Administració i Serveis del Parlament de Catalunya,

- Síndics de la Sindicatura de Comptes,
- Personal d'Administració i Serveis de la Sindicatura de Comptes,
- Síndic de Greuges,
- Personal d'Administració i serveis de la Sindicatura de Greuges
- Dispositius del Parlament de Catalunya.
- Personal assessor dels partits polítics o grups parlamentaris dintre de la infraestructura del Parlament de Catalunya

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, denominada "Arrel de la jerarquia pública de certificació de Catalunya" (<http://www.catcert.cat/descarrega/acc.crt>), que té com a finalitat la d'integrar d'altres

entitats de certificació en el sistema públic català de certificació, mitjançant la vinculació tècnica de les autoritats de certificació corresponents.

1.3.3 EC-PARLAMENT

El Parlament de Catalunya i el Consorci de l'Administració Oberta Electrònica de Catalunya varen signar en data 18 de juny de 2004, l'Acord Institucional d'impulsar l'ús de les tecnologies de la informació i de la comunicació i per a implantar nous serveis i instruments per a la tramitació telemàtica al Parlament de Catalunya. Dins els pactes adoptats a l'Acord Institucional esmentat, es va acordar la creació de l'Entitat de certificació "Parlament de Catalunya" (EC-PARLAMENT), vinculada a la jerarquia d'entitats de certificació públiques de Catalunya, els serveis a desenvolupar de la qual varen quedar reflectits en el Conveni de col·laboració subscrit pel Parlament de Catalunya i per l'Agència Catalana de Certificació, amb data 18 de juny de 2004.

L'EC-PARLAMENT és l'Entitat de Certificació del Parlament de Catalunya, operada per CATCert i vinculada a la jerarquia pública de certificació de Catalunya, que emet els certificats indicats a la secció 1.1.1 de la present DPC.

L'EC-PARLAMENT, com a Entitat de Certificació Virtual que gestiona la comunitat d'usuaris del Parlament de Catalunya, emet i gestiona els certificats d'usuari final de classe 1 i de classe 2, incloent-hi persones, dispositius i entitats.

1.3.4 Entitats de Registre

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

El procés de creació d'entitats de registre és responsabilitat de l'administrador de l'Entitat de Certificació. Les entitats de registre es poden constituir mitjançant acord de l'òrgan competent. Donat el cas, 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 tot examinant la sol·licitud i les dades incloses en el certificat de dades i fent totes les comprovacions necessàries per al compliment d'aquesta Política General de Certificació i de la Declaració de Pràctiques de Certificació.

El Parlament de Catalunya actua com a:

- Entitat de Registre, quan subscriu certificats de classe 1. Les Entitats de Registre corresponen a unitats o departaments subscriptors de certificats de classe 1 que operen un component tècnic de la infraestructura de claus públiques denominada Autoritat de Registre Local, que serveix per a identificar als posseïdors de claus, i tanmateix per a produir certificats i targetes per als posseïdors de claus i fer-los entrega d'aquests elements.

Tanmateix, disposa d'una Autoritat de Registre Remota per a generar les sol·licituds de certificats, podent també tramitar les sol·licituds tramitades per a organitzacions amb la citada Autoritat.

- Entitat de Registre, quan assisteix a les Institucions subscriptores de certificats de classe 1 i quan col·labora amb l' EC-PARLAMENT en el procés de emissió de certificats de classe 2.

En qualsevol cas, el Parlament de Catalunya dissenya i implanta els components i procediments tècnics, jurídics i de seguretat, referents al cicle de vida de:

- els dispositius segurs de creació de signatura o, en el seu cas, xifrat,
- les claus, i
- els certificats que emet

1.3.5 Usuaris finals

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

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

1.3.5.1 Sol·licitants de certificats

Els sol·licitants dels certificats indicats a la present DPC són les persones autoritzades pel Parlament de Catalunya.

Poden ser sol·licitants:

- La persona que serà el futur subscriptor o posseïdor de claus
- Una persona autoritzada per l'EC-PARLAMENT

L'autorització podrà realitzar-se de forma expressa o tàcita i, en aquells casos en els que l'EC-PARLAMENT ho consideri convenient, haurà formalitzar-se documentalment.

1.3.5.2 Subscriptors de certificats

Els subscriptors dels certificats són les persones, físiques o jurídiques, identificades en el camp "Subject" del certificat. En certificats de dispositiu, en el camp "Subject" també s'identifica el dispositiu corresponent.

El subscriptor dels certificats de classe 1 és, bé el Parlament de Catalunya, bé institucions dependents orgànicament o funcionalment d'aquest, com ara la Sindicatura de Comptes, entre d'altres.

Tanmateix, està prevista la subscripció de certificats de classe 2 individuals per al personal assessor dels partits polítics o grups parlamentaris dintre de la infraestructura del Parlament de Catalunya.

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 personals o d'entitat, de classe 1 o 2 d'organització, i que es troben degudament autoritzades a tal efecte pel subscriptor i degudament identificades en el certificat mitjançant el seu nom i cognoms o mitjançant un pseudònim (possibilitat aquesta última únicament aplicable als certificats de classe 2).

En els certificats d'entitat, a més, els posseïdors de claus han de tenir en compte allò que s'estableix a l'article 7 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, especialment en allò relatiu a la transgressió dels límits d'ús dels certificats.

Els posseïdors de claus dels certificats de classe 1 emesos per l'EC-PARLAMENT són els parlamentaris i el personal d'administració i serveis del Parlament de Catalunya, així com els Síndics i el personal d'administració i serveis de la Sindicatura de Comptes.

Els posseïdors de claus dels certificats de classe 2 emesos per l'EC-PARLAMENT són el personal assessor dels partits polítics o grups parlamentaris dintre de la infraestructura del Parlament de Catalunya.

1.3.5.4 Verificadors de certificats

Els verificadors són les persones (incloent-hi persones físiques, institucions, persones jurídiques i d'altres organitzacions i entitats) que reben signatures electròniques, segells electrònics i certificats digitals i han de verificar-les, com a pas previ a confiar en les mateixes.

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

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

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

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

1.4 Ús dels certificats

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

1.4.1 Usos típics dels certificats

1.4.1.1. Certificats d'infraestructura

1.4.1.1.1. Certificat d'infraestructura personal d'identificació i signatura reconeguda (CIPISR)

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

Els certificats d'infraestructura d'identificació i signatura 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 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'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, CPISR, CIDS, CIDA, CIO, CIV, CIT, 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, amb càrrec (CPISR-1 amb Càrrec)

Els certificats personals d'identificació i signatura reconeguda són certificats reconeguts d'acord amb allò que estableix l'article 11.1, amb el contingut prescrit per l'article 11.2 i emesos complint amb 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 a allò que disposa la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Els CPISR-1 amb càrrec, 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, de signatura electrònica.

Per aquest motiu, els CPISR-1 amb càrrec, 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 3.4 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, 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, d'acord amb aquesta Declaració de pràctiques.

Tanmateix, els CPISR-1 amb càrrec, es poden utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura escrita, sinó únicament la identificació del posseïdor de claus, entre els quals es poden indicar els següents:

- Autenticació en sistemes de control d'accés
- Signatura de correu electrònic segur
- Altres aplicacions de la signatura digital

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

Els certificats personals d'identificació i signatura reconeguda amb càrrec per a ús concret són certificats reconeguts d'acord amb allò que estableix l'article 11.1, amb el contingut prescrit per l'article 11.2 i emesos complint amb 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 a allò que disposa 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 3.4 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, 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, d'acord amb aquesta Declaració de pràctiques. A més de la persona que el posseeix, identifica l'organització subscriptora i el càrrec del posseïdor en aquesta i les limitacions materials d'ús.

Tanmateix, els CPISR-1 Càrrec Ús, es poden utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura escrita, sinó únicament la identificació del posseïdor de claus, entre els quals es poden indicar els següents:

- Autenticació en sistemes de control d'accés
- Signatura de correu electrònic segur
- Altres aplicacions de la signatura digital

1.4.1.2.3. Certificats personals d'identificació i signatura electrònica reconeguda de classe 2 amb càrrec, (CPISR-2 càrrec)

Els certificats personals d'identificació i signatura reconeguda de classe 2 amb càrrec 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 amb 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 a allò que es disposa per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Els CPISR-2 càrrec 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, de signatura electrònica.

Per aquest motiu, els CPISR-2 càrrec 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 3.4 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, s'equipara a la signatura escrita per efecte legal, sense necessitat de complir cap altre requeriment addicional.

Per últim, els CPISR-2 càrrec, es poden utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura escrita, sinó únicament la identificació del posseïdor de claus, entre els quals es poden indicar els següents:

- Autenticació en sistemes de control d'accés
- Signatura de correu electrònic segur
- Altres aplicacions de signatura digital

1.4.1.2.4. Certificats personals de xifrat de classe 1 amb càrrec (CPX-1 amb 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 donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Es tracta d'un certifica 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 es poden utilitzar exclusivament per a rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, per part del remitent del missatge, emprant:

- La clau pública del posseïdor de claus indicada en el certificat CPX-1 amb Càrrec.
- Una clau de xifrat de sessió, simètrica, xifrada amb la clau pública del posseïdor de claus indicada en el propi certificat CPX-1 amb Càrrec.

El posseïdor de la clau utilitza la seva clau privada per a desxifrar el missatge.

Els certificats CPX-1 amb Càrrec garanteixen la identitat del subscriptor, però no en permeten la signatura electrònica de missatges de dades.

La clau privada dels certificats CPX-1 amb Càrrec ha d'estar arxivada per l'EC-PARLAMENT de manera que, en determinades circumstàncies, pugui recuperar-se i accedir a la informació xifrada, sense ni tan sols la intervenció del posseïdor de claus.

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

Es tracta d'un certifica 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, xifrat i signatura avançada amb càrrec d'empleat públic de classe 1 (CPIXSA-1 Càrrec EP)

El certificat personal d'identificació, xifrat i signatura avançada amb càrrec d'empleat públic de classe 1 és un certificat reconegut d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emès complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

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

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

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

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

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

1.4.1.3. Certificats d'Entitat

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

Els certificats d'entitat d'identificació amb signatura reconeguda de classe 1 són certificats reconeguts, no emesos al públic, d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emès complint les obligacions dels articles 7, 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i 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 de signatura, essent idonis per a oferir suport a la signatura electrònica reconeguda de l'entitat; és a dir, és la signatura electrònica avançada que es basa en un certificat reconegut i que ha estat generada utilitzant un dispositiu segur, per la qual cosa, d'acord amb el que estableix l'article 3.4 de la Llei 59/2003, de 19 de desembre, s'equipara a la signatura escrita per efecte legal, sense necessitat de complir cap altre requeriment addicional.

1.4.1.3.2. Certificats d'entitat de xifrat de classe 1 (CEX-1)

Els certificats d'entitat de xifrat de classe 1 són certificats no reconeguts, no emesos al públic, que s'expedeixen a subscriptors i que es poden utilitzar exclusivament per a 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 en el propi certificat CEX.

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

El posseïdor de la clau utilitza la seva clau privada per a desxifrar el missatge. 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 certificats de dispositiu de servidor segur (CDS) s'emeten a les persones físiques o jurídiques responsables de la operació de servidors segurs SSL o TLS, amb els següents usos:

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

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

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

Els CDS-1 EV s'emeten a les Institucions, responsables de l'operació de servidors segurs SSL o TLS, amb els següents usos:

- Autenticació de servidor
- Xifrat de les comunicacions entre client i servidor
- Validació automàtica del certificat mitjançant els navegadors web adherits a CABForum.

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

1.4.1.4.2. Certificats de dispositiu d'aplicació digitalment assegurada de classe 1 (CDA-1)

Els certificats de dispositiu d'aplicació digitalment assegurada (CDA) s'emeten a les persones autoritzades pel Parlament de Catalunya, responsables de la operació d'aplicacions informàtiques que s'identifiquen digitalment, signen electrònicament *webservices* o d'altres protocols i que reben documents i missatges xifrats.

Els certificats CDA són certificats ordinaris, que garanteixen la identitat de la persona responsable i la integritat i l'autenticitat de les dades signades. Tanmateix, els certificats CDA permeten la recepció d'informació xifrada.

1.4.1.4.3. Certificats de dispositiu software o de signatura d'aplicacions informàtiques de classe 1 (CDP-1)

Els certificats de dispositiu software o de signatura d'aplicacions informàtiques (CDP) s'emeten a les persones autoritzades pel Parlament de Catalunya, responsables de l'edició, publicació o distribució digitals de software informàtic per a la signatura del software, que permet instal·lar-lo o executar-lo a distància.

Els certificats CDP són certificats ordinaris, que garanteixen la identitat de la persona responsable i l'origen i la integritat del software signat.

1.4.1.4.4. Certificats de dispositiu segur de controlador de dominis (CDSCD)

Els certificats de dispositiu segur de controlador de dominis (CDSCD) són emesos a les persones autoritzades pel Parlament de Catalunya, responsables de la operació de controlador de dominis, amb els següents usos:

- Autenticació de servidor
- Xifrat dels usuaris amb targeta criptogràfica.

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

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

Els CDS-1 Seu electrònica Extended Validation 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 software 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.

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

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

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

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

1.4.2. Aplicacions prohibides

1.4.2.1. Aplicacions prohibides per a tots els tipus de certificats

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

1.4.2.2. Certificats d'infraestructura

1.4.2.2.1. 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. Aplicacions prohibides per als certificats personals d'identificació i signatura electrònica reconeguda.

Els certificats CIPISR-1 amb Càrrec, CIPISR-1 Càrrec Ús i CIPISR-2 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 tampoc llistes de revocació de certificats (LRC).
- Xifrar ni desxifrar missatges o documents.

1.4.2.3.2. Aplicacions prohibides per als certificats personals de xifrat

Els certificats CPX-1 amb Càrrec i CPX-2 Càrrec no es poden utilitzar per a generar signatures electròniques de cap tipus de missatge de dades.

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

Els certificats CPIXSA-1 Càrrec EP no es poden utilitzar per a:

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

1.4.2.4. Certificats d'entitat

1.4.2.4.1. Aplicacions prohibides per als certificats d'entitat d'identificació i signatura electrònica reconeguda

Els certificats CEISR no es poden utilitzar per a:

- Signar sol·licituds 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. Aplicacions prohibides per als certificats d'entitat de xifrat

Els certificats CEX no es poden utilitzar per a 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. Certificat de dispositiu de servidor segur

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

1.4.2.5.2. Certificat de dispositiu de servidor segur seu electrònica

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

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

Els CDA-1 Segell electrònic no es poden utilitzar per a la realització d'actes manuals.

1.4.2.5.3. Aplicacions prohibides per als certificats de dispositiu de servidor segur

Els certificats CDS no es poden utilitzar per a:

- Signar sol·licituds d'emissió, renovació, suspensió o revocació de certificats CIC.
- Signar certificats de cap tipus o llistes de revocació de certificats (LRC).

1.4.2.5.4. Aplicacions prohibides per als certificats d'aplicació digitalment assegurada

Els certificats CDA no es poden utilitzar per a:

- Signar sol·licituds d'emissió, renovació, suspensió o revocació de certificats CIC, ni de cap altre tipus.
- Signar llistes de revocació de certificats (LRC)

- Assegurar aplicacions diferents a la identificada en el certificat.

1.4.2.5.5. Aplicacions prohibides per als certificats de dispositiu software o de signatura d'aplicacions informàtiques (CDP)

Els certificats CDP no es poden utilitzar per a:

- Signar sol·licituds d'emissió, renovació, suspensió o revocació de certificats CIC, ni de cap altre tipus.
- Signar llistes de revocació de certificats (LRC)
- Assegurar software diferent a aquell identificat en el certificat.
-

1.4.2.5.6. Aplicacions prohibides per als certificats de dispositiu segur de controlador de dominis (CDSCD)

Els certificats CDSCD no es poden utilitzar per a:

- Signar sol·licituds d'emissió, renovació, suspensió o revocació de certificats CIC.
- Signar certificats de cap tipus o llistes de revocació de certificats (LRC).
-

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.cat Telèfon assistència: 902 901 080	Parlament de Catalunya Parc de la Ciutadella, s/n 08003 Barcelona 93 304 65 00
--	---

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	Parlament de Catalunya Parc de la Ciutadella, s/n 08003 Barcelona 93 304 65 00
---	---

Fax: 93 272 25 39 Correu electrònic: info@catcert.cat Telèfon assistència: 902 901 080	
---	--

1.5.3. Persona que determina la conformitat de la Declaració de Pràctiques de Certificació (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.cat Telèfon assistència: 902 901 080	Parlament de Catalunya Parc de la Ciutadella, s/n 08003 Barcelona 93 304 65 00
--	---

1.5.4. Procediment d'aprovació

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

Es preveu, d'aquesta manera, el procediment de modificació d'especificacions del servei i el procediment de publicació d'especificacions del 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, els 7 dies de la setmana i, en cas de fallida del sistema, per causes alienes al control de l'EC-PARLAMENT, aquesta realitza els seus millors esforços per a que el servei estigui disponible de nou en el terme establert a la secció 5.7.4 de la present DPC.

2.2. Publicació d'informació de l'EC-PARLAMENT

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

- a) Les llistes de certificats revocats i d'altres informacions d'estat de revocació dels certificats.
- b) La política general de certificació i, quan resulti convenient, les polítiques específiques.
- 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 l'EC-PARLAMENT.

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 substituïda per la nova versió.

2.3. Freqüència de publicació

La informació de l'EC-PARLAMENT 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 de la present DPC es regeixen per allò establert a la secció 9.12.1.

La informació d'estat de revocació de certificats es publica d'acord amb allò establert a la secció 4.9.7 de la present DPC.

Transcorreguts quinze (15) 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 quinze (15) anys per l'EC-PARLAMENT, podent ésser consultades, per causa raonada, pels interessats.

2.4. Control d'accés

L'EC-PARLAMENT no limita l'accés de lectura a les informacions del Directori, però estableix controls per a 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-PARLAMENT 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.
- Es detecti qualsevol canvi tècnic que afecti als 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 ha de realitzar-se amb anterioritat a l'emissió i entrega de certificats.

3.1.1. Tipus de noms

3.1.1.1. Estructura sintàctica

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

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

3.1.1.2. Perfils dels certificats

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

3.1.2. Significat dels noms

En els certificats personals la identificació de les persones físiques (posseïdores de claus) està formada pel seu nom i cognoms, més el seu NIF o NIE, de conformitat amb la secció 3.1.6 de la present DPC.

La identificació de les persones jurídiques (subscriptores) està formada per la seva denominació o raó social, més el seu CIF.

3.1.3. Utilització d'anònims i pseudònims

No es poden utilitzar pseudònims per a identificar a una organització.

3.1.4. Interpretació de formats de noms

Sense estipulació addicional.

3.1.5. Unicitat dels noms

L'EC-PARLAMENT emet diferents tipus de certificats. Els noms dels subscriptors de certificats són únics, per a cada servei de generació de certificats opera per l'EC-PARLAMENT i per a cada tipus de certificat; és a dir, una mateixa persona només pot tenir al seu nom certificats de tipus diferents emesos per l'EC-PARLAMENT.

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-PARLAMENT 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.

D'igual forma, l'EC-PARLAMENT no actua com a àrbitre o mediador, ni de cap altra manera resol cap disputa referent a la propietat de noms de persones o organitzacions, noms de domini, marques o noms comercials (per exemple relatius a adreces de correu electrònic).

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

Els conflictes de noms de posseïdors de claus que apareixen identificats en els **certificats personals de classe 1** amb el seu nom real es solucionen mitjançant la inclusió, en el nom diferenciat del certificat:

- En cas de nacionals espanyols, el DNI del posseïdor de claus.
V.gr.: (C) = ES; (SN) = DNI
 - En cas d'estrangers amb algun tipus de vinculació amb Espanya, com pot ésser la residència en territori espanyol, el NIE del posseïdor de claus.
V.gr.: francès (C) = ES; (SN) = NIE
V.gr.: argentí (C) = ES; (SN) = NIE
 - En cas d'estrangers nacionals d'Estats part de l'Acord Schengen i mancats de NIE, el document nacional d'identitat del país d'origen o de procedència o passaport vigent del posseïdor de claus.
V.gr.: italià (C) = ES; (SN) = IT-Document nacional d'identitat
 - En cas d'estrangers nacionals d'Estats que no són part de l'Acord Schengen i mancats de NIE, el Passaport ordinari, diplomàtic, oficial o de servei, del posseïdor de claus vàlidament expedit i en vigor.
V.gr.: xinès (C) = ES; (SN) = CN-Passaport
- En els dos supòsits anteriors, juntament amb els identificadors assenyalats 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).
- Qualsevol altre identificador assignat al posseïdor de claus pel subscriptor.

V.gr.: un número de carnet.

Aquest sistema de resolució de conflictes de noms respon al fet que tant el Parlament de Catalunya com les Institucions dependents orgànicament d'aquest, identificades en els certificats de classe 1 en el camp "Organizational Unit Name" del "Subject" del perfil com a subscriptores, estan sotmeses a Dret espanyol.

La submissió al Dret espanyol ve determinada per la RFC 3739, que estableix que el camp "Subject" contindrà, entre d'altres atributs, l'atribut "countryName" el valor del qual consisteix en especificar el context en el que s'han d'entendre definits els altres atributs del "Subject", entre els quals es troba el "Serial Number".

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

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

Aquells estrangers mancats de NIE, s'identifiquen amb la corresponent documentació acreditativa, que varia en funció de la seva nacionalitat, diferenciant-se entre els nacionals d'Estat part de l'Acord Schengen i els altres. Els primers acrediten la seva identitat mitjançant la presentació del seu document nacional d'identitat o del seu passaport vàlidament expedit i en vigor. Els segons l'acrediten mitjançant el passaport, el títol de viatge o el document nacional d'identitat o cèdula d'identificació o qualsevol altre document que acrediti la seva identitat en virtut de compromisos internacionals, en els que quedi perfectament reflectida la identitat i la nacionalitat del titular del document.

Els conflictes de noms de subscriptors que apareixen identificats en els **certificats personals de classe 2 individuals** amb el seu nom real es solucionen mitjançant la inclusió, en el nom diferenciat del certificat:

- 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 en territori espanyol, el NIE del posseïdor de claus.
V.gr.: francès (C) = ES; (SN) = NIE
V.gr.: argentí (C) = ES; (SN) = NIE
- En cas d'estrangers nacionals d'Estat part de l'Acord Schengen i mancats 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 d'identitat
- En cas d'estrangers nacionals d'Estat que no són part de l'Acord Schengen i mancats 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, juntament amb els identificadors assenyalats es col·locarà el codi del país del que el subscriptor n'és nacional, separat per un guió, de conformitat amb els paràmetres establerts per la norma ISO 3166 Codes (Countries).

En **certificats d'entitat**, els conflictes de noms dels responsables de la custòdia de claus que apareixen identificats en els certificats amb el seu nom real es solucionen mitjançant la

inclusió, en el nom diferenciat del certificat, del DNI o NIE del responsable de la custòdia de claus.

En allò referent al tractament de marques registrades, s'estarà a allò que disposa l'apartat 9.5.3 de la present DPC.

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.

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-PARLAMENT 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-PARLAMENT utilitzarà algun dels següents mètodes:

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

3.2.2.2. Subscriptors de certificats

3.2.2.2.1. Requisits per a certificats de classe 1

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

3.2.2.2.2. Requisits per a certificats de classe 2

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

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

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

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

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

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

3.2.2.2.4. Requisits específics per al CDA i el CDA-1 Segell electrònic

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

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

3.2.2.2.5. Requisits específics per al CDP

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

- L'existència i la titularitat del software.

- L'autorització de l'organització per a l'emissió del certificat en el dispositiu corresponent.

3.2.3. Autenticació de la identitat d'una persona física

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

3.2.3.1. Elements d'identificació requerits

El número i tipus de documents necessaris per a acreditar la identitat del posseïdor de claus són els que admet l'EC-PARLAMENT tal i com es recull a la seva normativa específica reguladora.

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

- Nom i cognoms de la persona
- Número d'identitat reconegut legalment (DNI, NIF o NIE dels països signataris de l'Acord Schengen; passaport en el cas dels certificats d'estranger).
- Altres atributs de la persona que hagin de constar en el certificat, que puguin ser utilitzats per a diferenciar a una persona d'una altra, dintre de l'àmbit del Parlament de Catalunya (per exemple, fotografia, adreça de correu electrònic, categoria, càrrec, etc.)

3.2.3.2. Validació dels elements d'identificació

La informació d'identificació de posseïdors de claus de certificats de classes 1 i 2 es valida comparant la informació de la sol·licitud amb els registres interns de l'Entitat de Registre en el cas dels certificats de classe 1 o amb la documentació aportada, electrònicament o en suport físic, en els certificats de classe 2.

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

La informació del posseïdor registrada pel Parlament de Catalunya en els últims cinc anys està actualitzada.

3.2.3.3. Necessitat de presència personal

És necessari validar la identitat del posseïdor de claus o del responsable de la custòdia amb la seva presència física, que és responsabilitat del propi Parlament de Catalunya, qui ho fa mitjançant la 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.

3.2.4. Informació no verificada

L'EC-PARLAMENT es responsabilitza de que tota la informació inclosa a la sol·licitud del certificat és exacta i completa per a la finalitat del certificat.

No obstant l'anterior, els certificats poden incloure informació no verificada, com per exemple l'adreça de correu electrònic, sempre que s'indiqui als usuaris finals en el mateix certificat o en els instruments jurídics corresponents.

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, s'hauran d'enregistrar adequadament els canvis que s'hagin pogut produir. Si més no, si la renovació es realitza durant els 5 primers anys des de la primera comprovació de la identitat, dita identificació no serà necessària.

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

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

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

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

4.1. Sol·licitud d'emissió de certificat

4.1.1. Legitimació per a sol·licitar l'emissió

4.1.1.1 Requisits 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 o 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, quan escaigui.

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 per a tots tipus de 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 amb signatura manuscrita 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-PARLAMENT 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-PARLAMENT 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-PARLAMENT, 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.Requisits addicionals per al CDS-1, CDS-1 EV, el CDSCD-1 i el CDS-1 Seu electrònica EV

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

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

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

4.2.4.Requisits específics per al CIPISR

. Addicionalment, l'Entitat de Certificació haurà de:

- Incloure al certificat les informacions establertes a l'art. 11 de la Llei 59/2003, d'acord amb l'establert a la secció 7 d'aquesta política.

- Garantir la data i l'hora en què es va expedir un 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-PARLAMENT 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.

Després de l'aprovació de la sol·licitud de certificació es procedirà a l'emissió del certificat, de forma segura i es posarà el certificat a disposició del subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització o de entitat, per a la acceptació d'aquests, d'acord amb el que s'estableix a la secció corresponent.

Per a cada sol·licitud de certificat aprovada, l'EC-PARLAMENT ha de:

- Utilitzar un procediment de generació de certificats que vinculi de forma segura el certificat amb la informació de registre, incloent-hi la clau pública certificada
- En cas que l'Entitat de Certificació generi el parell de claus, utilitzar un procediment de generació de certificats vinculat de forma segura amb el procediment de generació de claus i, que la clau privada és lliurada de forma segura al subscriptor, en cas de certificats individuals, o al posseïdor de claus en cas de certificats d'organització.

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);

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

4.3.2. Notificació de l'emissió al subscriptor

L'EC-PARLAMENT notifica al subscriptor, en el cas de certificats individuals, o al futur posseïdor de claus, en cas de certificats d'organització o d'entitat, que el certificat ha estat emès, està disponible i la forma d'obtenir-lo.

4.4. Acceptació del certificat

4.4.1. Responsabilitats de l'EC-PARLAMENT

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.

L'EC-PARLAMENT 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 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.

L'EC-PARLAMENT 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 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 de classe 1 es poden publicar sense el consentiment previ dels posseïdors de claus.

Per contra, la publicació dels certificats de classe 2 requerirà sempre del consentiment del subscriptor.

4.4.4. Notificació de l'emissió a tercers

No aplicable.

4.5. Ús del parell de claus i del certificat

4.5.1. Ús del parell de claus pels posseïdors de claus i ús del certificat pels subscriptors

4.5.1.1. Requisits per a tots els tipus de certificats

Els certificats s'utilitzen per a permetre una millor seguretat en les comunicacions telemàtiques internes de les Institucions, tant entre elles, com les que 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 per a d'altres funcions o finalitats.

S'han d'utilitzar 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-les, generar signatures electròniques i, en el seu cas, desxifrar aquells missatges en què l'emissor ha decidit preservar el contingut.

L'extensió *Key Usage* s'utilitza per a establir límits tècnics als usos que poden 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, per contra, depenen en ocasions de l'operació d'aplicacions informàtiques que no han estat fabricades ni poden estar controlades per l'EC-PARLAMENT.

4.5.1.2. Informacions addicionals per als certificats personals

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

4.5.1.3. Informacions addicionals per al CIPISR

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

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

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

4.5.1.4. Informacions addicionals per al CPISR

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

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

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

4.5.1.5. Informacions addicionals per al CPIXSA

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

4.5.1.6. 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.

4.5.1.7. 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.

4.5.1.8. 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.

4.5.1.9. Informacions addicionals per al CEIXSA

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

4.5.1.10. Informacions addicionals per al CDS-1 i el CDS-1 EV

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

4.5.2. Ús pel tercer que confia en certificats

Els certificats s'utilitzen d'acord amb la seva funció pròpia i finalitat establerta, sense que puguin ser utilitzats en d'altres funcions i amb d'altres finalitzades. De la mateixa manera, 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 confiar en el seu contingut.

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

Tanmateix, s'ha de tenir en compte que es 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 l'EC-PARLAMENT.

4.6. Renovació de certificats sense renovació de claus

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

4.7. Renovació de certificats amb renovació de claus

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

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

4.8. Modificació de certificats

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

4.9. Revocació i suspensió de certificats

4.9.1. Causes de revocació de certificats

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

1. Circumstàncies que afecten a la informació continguda en el certificat
 - Modificació d'alguna de les dades contingudes en el certificat.
 - Descobriment que alguna de les dades contingudes a la sol·licitud de certificat és incorrecta.
 - Descobriment que alguna de les dades contingudes en el certificat és incorrecta.
2. Circumstàncies que afecten a la seguretat de la clau o del certificat
 - Compromís de la clau privada o de la infraestructura o sistemes de l'EC-PARLAMENT, sempre que afecti a la confiança en els certificats emesos a partir d'aquest incident.
 - Infracció, per l'EC-PARLAMENT, dels requisits previstos en els procediments de gestió de certificats.
 - Compromís o sospita de compromís de la seguretat de la clau o del certificat del subscriptor.
 - Accés o utilització no autoritzada, per un tercer, de la clau privada del subscriptor.
 - Ús irregular del certificat pel subscriptor o falta de diligència en la custòdia de la clau privada.
3. Circumstàncies que afecten al 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 al subscriptor o al posseïdor de claus
 - Fi de la relació entre el Parlament de Catalunya i el posseïdor de claus.
 - Modificació o extinció de la relació jurídica subjacent o causa que va provocar l'emissió del certificat.

- Infracció per part del sol·licitant del certificat dels requisits preestablerts per a la sol·licitud d'aquest.
- Infracció pel subscriptor de les seves obligacions, responsabilitat i garanties, establertes a l'instrument jurídic corresponent de l'EC-PARLAMENT.
- L'extinció de la persona jurídica subscriptora del certificat, així com la finalitat de l'autorització del subscriptor al posseïdor de claus o la fi 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-PARLAMENT, d'acord amb l'establert a la secció 5.8 d'aquest document.
- La finalització de prestació de serveis per part de CATCert, d'acord amb el que estableix la Política General de Certificació.
- Resolució judicial o administrativa que ho ordeni (Art. 8.1 de la Llei 59/2003, de signatura electrònica).
- L'EC-PARLAMENT té coneixement que els CDP han realitzat signatures sobre codi hostil.

Si l'EC-PARLAMENT no disposa de tota la informació necessària per a 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-PARLAMENT 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 esmentades anteriorment.

4.9.2. Legitimació per a sol·licitar la revocació

La sol·licitud de revocació es realitza per pel subscriptor del certificat, CATCert, 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, que accedeix a l'aplicació web, mitjançant un certificat d'operador, de classe 1 o de classe 2, en funció de si és un operador de l'Entitat de Registre o un operador del Centre de Trucades, emès per CATCert, i a continuació i de forma automàtica i immediata s'indica l'esmentada revocació en l'estat del certificat en la llista de revocacions.

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

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

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

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

L'EC-PARLAMENT 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 remetran de forma raonablement immediata quan es tingui coneixement de la causa de revocació.

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

La sol·licitud de revocació és processada en el mínim termini possible.

4.9.6.Obligació de consulta d'informació de revocació de certificats

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

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

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

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

L'EC-PARLAMENT 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 (<http://www.catcert.cat/>).

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

Els serveis de comprovació d'estat de certificats es troben disponibles les 24 hores del dia, els 7 dies de la setmana.

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

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

Els verificadors han de comprovar l'estat d'aquells certificats en els que desitja confiar.

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

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

4.9.11. Altres formes d'informació de revocació de certificats

L'EC-PARLAMENT també informará sobre la revocació dels certificats, mitjançant el protocol OSCP, 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 OSCP retornará una resposta que identifiqui el motiu pel qual no es torna aquesta resposta (sol·licitant no autoritzat, error en la resposta o inoperabilitat temporal del prestador requerit).

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

Aquesta resposta es signarà 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-PARLAMENT és notificat, en la mesura del possible, a tots els participants de la jerarquia pública de certificació de Catalunya, mitjançant el Dipòsit de CATCert.

4.9.13. Causes de suspensió de certificats

Els certificats de l'EC-PARLAMENT es poden suspendre en els següents casos:

- Quan ho sol·liciti el posseïdor de claus o el subscriptor o un tercer autoritzat (art. 9.1.a de la Llei 59/2003)
- En els casos legals previstos a l'article 9.1 de la Llei de Signatura Electrònica, és a dir, en cas que una resolució judicial o administrativa ho ordeni.
- Quan així sigui sol·licitat pel subscriptor o posseïdor de claus.
- Quan la documentació requerida a la sol·licitud de revocació sigui suficient però no es pugui identificar raonablement al posseïdor de claus.
- Quan la documentació requerida a la sol·licitud de revocació no sigui suficient, encara que es pugui identificar raonablement al posseïdor de claus.
- Quan la documentació requerida a la sol·licitud de revocació no sigui suficient i tampoc permeti identificar raonablement al posseïdor de claus.
- La falta d'ús del certificat durant un període llarg de temps, conegut prèviament.

- Si se sospita del compromís d'una clau, fins que aquest hagi estat confirmat. En aquest segon cas, l'EC-PARLAMENT ha d'assegurar-se de que el certificat no està suspès durant més temps del necessari per a 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. L'EC-PARLAMENT.

4.9.15. Procediments de sol·licitud de suspensió

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

1. La suspensió pot ser sol·licitada pel posseïdor de les claus i es pot dur a terme per via telefònica al 902 90 10 80.
2. La suspensió pot ser sol·licitada pel subscriptor del certificat i es pot realitzar per via telefònica al 902 90 10 80.
3. La suspensió pot ser realitzada per l'EC-PARLAMENT directament, a través del component LRA o RRA.

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

Per iniciar la suspensió es requereix la següent informació:

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

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

4.9.16. Període màxim de suspensió

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

4.9.17. Habilitació d'un certificat suspès

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

4.10. Serveis de comprovació d'estat de certificats

4.10.1. Característiques d'operació dels serveis

Les LRC seran descarregades manualment des del directori 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 de fallida dels sistemes de comprovació d'estat dels certificats per causes fora del control de l'EC-PARLAMENT, aquesta realitza els seus millors esforços per a assegurar que aquest servei es manté inactiu el mínim temps possible. L'EC-PARLAMENT detalla a l'apartat 5.7.4 de la present DPC el màxim temps en el que el servei haurà de tornar a operar.

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

4.10.3. Altres funcions dels serveis

Sense estipulació addicional.

4.11. Acabament de la subscripció

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

4.12. Dipòsit i recuperació de claus

4.12.1 Política i pràctiques de dipòsit i recuperació de claus

No es practica recuperació de claus per als certificats CEIXSA.

La recuperació de claus de la resta de certificats de xifrat la realitza CATCert a instància de l'EC-PARLAMENT, que realitza mitjançant els seus procediments operatius. A aquest

efecte, el procediment operatiu corresponent designa els rols que hauran d'intervenir en aquesta operació i que seran objecte de designació en l'entitat que realitzi l'operació

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

Un cop s'han recuperat de la base de dades del servei KeyRecovery de la CA tant l'arxiu PKCS#12 com el password, s'enviaran al Generador mitjançant email xifrat i signat. El Generador haurà d'inserir el certificat en una targeta nova en cas que l'antiga no estiguis 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-PARLAMENT s'assegura de l'aplicació dels procediments administratius i de gestió, adequats i conformes amb els estàndards reconeguts i, en particular:

- a. Realitza una anàlisi de gestió de risc per a avaluar les necessàries mesures de seguretat.
- b. És responsable per la provisió dels serveis de forma segura, inclòs quan una part dels mateixos és subcontractada. Les responsabilitats de tercers són definides i s'han d'implantar els necessaris controls jurídics a fi i efecte de garantir que els tercers compleixen amb les seves obligacions amb un nivell de seguretat equivalent.
- 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 a gestionar la seguretat de les operacions. Qualsevol canvi que tingui impacte en el nivell de seguretat ha de ser aprovat per l'òrgan referit en el número anterior.
- e. Es documenten, implanten i mantenen els controls de seguretat i procediments d'operació de les instal·lacions, sistemes i actius d'informació en que se sustenta la prestació dels serveis.
- f. En cas de subcontractació total dels serveis, es garanteix el manteniment del necessari nivell de seguretat de la informació.

5.1. Controls de seguretat física

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

Igualment, les Entitats de Registre que generin certificats dins de dispositius segurs de creació de signatura o d'altres mòduls de seguretat criptogràfica també disposen d'equivalents mesures de seguretat física, que són aprovades per l'EC-PARLAMENT 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-PARLAMENT i les Entitats de Registre estableixen controls de seguretat física i ambientals per protegir els recursos de les instal·lacions on es troben els sistemes, els mateixos sistemes i els equipaments utilitzats per a les operacions. La política de seguretat física i ambiental aplicable als serveis de generació de certificats, de dispositius criptogràfics i de gestió del cicle de vida estableix prescripcions per a les següents contingències:

- Controls d'accés físic
- Protecció davant de desastres naturals
- Mesures de protecció davant d'incendis

- Error dels sistemes de suport (energia elèctrica, telecomunicacions, etc.)
- Demolició de l'estructura
- Inundacions
- Protecció antirobatoris
- Conformitat i entrada no autoritzada
- Recuperació del desastre
- Sortida no autoritzada d'equipaments, informacions, suports i aplicacions relatius a components utilitzats per als serveis de l'EC-PARLAMENT.

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-PARLAMENT).

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-PARLAMENT 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-PARLAMENT 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-PARLAMENT, 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-PARLAMENT 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-PARLAMENT 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-PARLAMENT compten amb sistemes automàtics de detecció i extinció d'incendis.

En concret, els dispositius criptogràfics i suports que emmagatzemen claus de les Entitats de Certificació han de disposar d'un sistema específic i addicional a la resta de la instal·lació, per a la protecció davant del foc.

5.1.6. Emmagatzematge de suports

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

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

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

Cal tenir en compte que les entitats de registre es queden amb una còpia signada pel posseïdor de claus del full de lliurament de certificats. Aquesta còpia es guardada durant 15 anys per l'Entitat de Registre, aplicant-li allò que indica la legislació catalana d'arxius, en relació amb la guarda i custòdia de documentació.

5.1.7. Tractament de residus

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

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

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

5.1.8. Còpia de seguretat fora de les instal·lacions

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

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

En el moment de realitzar una sortida d'informació de les dependències s'adopten mesures adients per a impedir qualsevol recuperació indeguda de l'esmentada informació (com per

exemple, la utilització de carteres amb dispositius segurs de claus o combinacions, o la utilització de fitxers encriptats).

5.2. Controls de procediments

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

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

5.2.1. Funcions fiables

Les persones que ocupen aquestes posicions són formalment nomenats per l'alta direcció de l'EC-PARLAMENT.

Les funcions fiables inclouen:

- Personal responsable de la seguretat
- Administradors del sistema
- Operadors del sistema
- Operadors de registre
- 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 de la present DPC.

5.2.2. Nombre de persones per tasca

Les funcions fiables identificades a la política de seguretat de l'EC-PARLAMENT, 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-PARLAMENT identifica i autèntica el personal abans d'accedir a la corresponent funció fiable.

5.2.4. Rols que requereixen separació de tasques

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

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

- a. Deures associats a la funció

- b. Nivell d'accés
- c. Monitoratge de la funció
- d. Formació i conscienciació
- e. Habilitats requerides

Les citades restriccions s'apliquen en tot cas:

- a. La persona que actua com a oficial de seguretat o com a operador de registre no pot ser auditor del sistema.
- b. La persona que actua com a administrador del sistema no pot ser oficial de seguretat ni auditor del sistema.
- c. Quan el registre és practicat per una Entitat de Registre amb presència física del posseïdor de claus, l'oficial de registre pot aprovar i generar el certificat, mentre que en la resta de casos, i especialment quan el registre es practica de forma delegada per una Entitat de Registre, serà imprescindible segregar els rols d'aprovador i generador (gaudint tots dos de la consideració d'operadors de registre).

5.3. Controls de personal

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

- Es manté confidencialitat de la informació, posant els medis 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 a la política, als plans de seguretat o a la present DPC.
- 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 limita la qualitat del servei.
- S'utilitzen els actius de la infraestructura per a les finalitats que els hi han estat encarregades.
- 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 les que està sotmès.
- El Responsable de Seguretat vetlla per a que el punt anterior sigui executat, proveint als responsables d'àrea tota la informació que sigui necessària.
- No s'instal·la cap dels sistemes de la infraestructura, software o hardware que no sigui expressament autoritzat per escrit pel responsable de sistemes d'informació.
- No s'accedeix voluntàriament, ni s'elimina o altera informació no destinada a la seva persona o perfil professional.

El personal afectat per aquesta normativa és:

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

CATCert, a més a més, es veu afectada pel següent personal:

- qui fa les sol·licituds dels certificats
- qui fa l'aprovació i validació de les sol·licituds 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) involucrat en l'operació
- el responsable del servei.

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

L'EC-PARLAMENT 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 adequada.

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

La qualificació i l'experiència es poden suplir mitjançant una formació i entrenament adequats.

El personal en posicions fiables es trobarà lliure d'interessos personals que entrin en conflicte amb el desenvolupament de la funció que tingui encarregada.

5.3.2. Requisits de formació

L'EC-PARLAMENT 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 maquinaria i aplicacions en ús
- Tasques que ha de realitzar 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 a més, proporciona a tot el personal involucrat en les seves operacions com a 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 impartit per CATCert.

5.3.4. Seqüència i freqüència de rotació laboral

Sense estipulació addicional.

5.3.5. Sancions per accions no autoritzades

L'EC-PARLAMENT disposa d'un sistema sancionador, per a depurar 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-PARLAMENT contracta professionals per a qualsevol funció, inclòs per a un lloc fiable, cas en el que es 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 realitzades en aquesta secció 5, o en d'altres parts de la política de certificat o d'aquesta DPC, seran aplicades i completades pel tercer que realitza les funcions d'operació dels serveis de certificació. L'EC-PARLAMENT és responsable, en tot cas, de l'efectiva execució.

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

5.3.7. Subministrament de documentació al personal

L'EC-PARLAMENT subministra la documentació que estrictament necessiti el seu personal en cada moment, a fi i efecte que sigui suficientment competent.

5.4. Procediments d'auditoria de seguretat

5.4.1. Tipus d'esdeveniments registrats

L'EC-PARLAMENT guarda registre de, com a mínim, els següents esdeveniments relacionats amb la seguretat de l'Entitat:

- Encès i apagat dels sistemes
- L'inici i finalització de l'aplicació d'Autoritat (tècnica) de certificació
- Els intents de crear, esborrar, canviar contrasenyes o permisos dels usuaris dintre del sistema
- Els canvis en les claus de l'Autoritat (tècnica) de certificat
- Els canvis en les polítiques d'emissió de certificats
- Els intents d'entrada i sortida del sistema
- Els intents no autoritzats d'entrada a la xarxa de l'EC-PARLAMENT
- Els intents no autoritzats d'accés als fitxers del sistema
- La generació de les claus de l'EC-PARLAMENT
- Els 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-PARLAMENT també guarda, ja sigui manualment o electrònic, 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-PARLAMENT
- Informes complets dels intents d'intrusió física a 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 al menys una vegada a la setmana per buscar activitat sospitosa o no habitual.

El processament dels registres d'auditoria consisteixen 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 es trobaran documentades.

5.4.3. Període de conservació de registres d'auditoria

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

5.4.4. Protecció dels registres d'auditoria

Els fitxers de registres, tant manuals com electrònics, es protegeixen de lectures, modificacions, esborrats o qualsevol altre tipus de manipulació no autoritzada emprant controls d'accés lògic i físic, mitjançant les mesures de seguretat indicades a la secció 5 de la present DPC.

5.4.5. Procediments de còpies de seguretat

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

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

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

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

El sistema d'acumulació de registres d'auditoria és, al menys, un sistema intern de l'EC-PARLAMENT, compost pels registres de l'aplicació, pels registres de xarxa i pels registres del sistema operatiu, a més 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 a monitoritzar les vulnerabilitats del sistema.

Els anàlisis de vulnerabilitat són executats, repassats i revisats per mitjà d'un examen d'aquests esdeveniments monitoritzats

Aquests anàlisis són executats diàriament, mensualment i anualment d'acord amb la seva definició en el Pla d'Auditoria de l'EC-PARLAMENT.

5.5. Arxiu d'informacions

L'EC-PARLAMENT garanteix que tota la informació relativa als certificats es guarda durant un període de temps apropiat, segons s'estableix a la secció 0 de la present DPC, i que es gestiona de conformitat amb el procediment d'arxiu aprovat.

5.5.1. Tipus d'esdeveniments registrats

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

L'EC-PARLAMENT guarda un registre del següent:

Documents originals:

- Formulari de sol·licitud de certificats
- Certificat de dades
- Full d'entrega de subscriptor de certificats

Fotocòpies de:

- Carta d'entrega de certificats

- Carta PIN i PUK.

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

L'EC-PARLAMENT 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-PARLAMENT:

- 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. Aquestes còpies les guarda CATCert a les seves instal·lacions.

5.5.5. Requisits de segellat de cautela de data i hora

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

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

Solament les persones autoritzades per l'EC-PARLAMENT tenen accés a les dades d'arxiu, tant si es troben a les mateixes instal·lacions de l'EC-PARLAMENT o a la seva ubicació externa.

5.6. Renovació de claus

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

5.7. Compromís de claus i recuperació de desastres

5.7.1. Procediment de gestió d'incidències i compromisos

L'EC-PARLAMENT 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-PARLAMENT iniciarà les gestions necessàries, segons els documents Pla de Seguretat, Pla d'Emergència i Pla d'Auditoria, per a possibilitar que el sistema torni al seu estat normal de funcionament.

5.7.3. Compromís de la clau privada de l'Entitat

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

En cas de compromís l'EC-PARLAMENT:

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

5.7.4. Desastre sobre les instal·lacions

L'EC-PARLAMENT desenvolupa, manté, prova i, si cal, executa un pla d'emergència en el cas de desastres, ja sigui per causes naturals o causats per l'home sobre les instal·lacions, que indica com s'han de restaurar els serveis dels Sistemes d'Informació. La ubicació dels sistemes de recuperació de desastres disposa de les proteccions físiques de seguretat detallades en el Pla de Seguretat.

L'EC-PARLAMENT és capaç de restaurar l'operació normal de la PKI en les 24 hores següents al desastre, i es poden, com a mínim, executar les següents accions:

- Revocació de certificats

- Publicació d'informació de revocació

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

5.8. Finalització del servei

5.8.1. EC-PARLAMENT

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

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

- Informa a tots els subscriptors i verificadors (no es requereix que l'EC-PARLAMENT tingui cap relació anterior amb terceres parts).
- Acaba tota autorització de subcontractacions que actuen en nom de l'EC-PARLAMENT en el procés d'emissió de certificats.
- Executa les tasques necessàries per a 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-PARLAMENT o les retira de l'ús.

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

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

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

5.8.2. Entitat de Registre

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

6. Controls de seguretat tècnica

L'EC-PARLAMENT utilitza sistemes i productes fiables, que estan protegits contra tota alteració i que garanteixen la seguretat tècnica i criptogràfica dels processos de certificació als quals 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 de signatura reconeguda

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

6.1.1.3. Informació per als certificats CPIXSA

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

6.1.1.4. Informació per als certificats de xifrat

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

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

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

La clau pública dels certificats CDS-1, CDS-1 EV i CDSCD-1 es genera sota la seva responsabilitat, per part de l'Entitat de Registre. La clau privada la genera la Institució que sol·licita el certificat.

6.1.1.5. Informació per als certificats CDS-1 Seu electrònica EV

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

6.1.1.6. Informació per als certificats CDA-1 Segell electrònic

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

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 CIPIR, CPIR, CEIR, 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 CEIXA

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

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

El mètode d'enviament de la clau pública a l'EC-PARLAMENT és PKCS #10, altra prova criptogràfica equivalent o qualsevol altre mètode aprovat per CATCert.

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

La clau de l'EC-PARLAMENT 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 la Agència Catalana de Certificació-CATCert) què és l'arrel de la jerarquia, es publica en el directori de l'EC-PARLAMENT, en forma de certificat auto signat, juntament amb una declaració referent a que la clau permet autenticar a l'EC-PARLAMENT.

S'estableixen mesures addicionals per a confiar en el certificat auto signat, tals com ara la comprovació de la petjada digital del certificat.

La clau pública de l'EC-PARLAMENT es publica en el directori de l'EC-PARLAMENT, en forma de certificat CIC signat per CATCert.

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

Adicionalment, en aplicacions S/MIME, el missatge de dades conté una cadena de certificats, incloent-hi certificats CIC amb les claus públiques de les Entitats de Certificació de la jerarquia, que d'aquesta manera són distribuïdes als usuaris.

6.1.5. Mides de claus

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

Les claus de tots els certificats emesos per l'EC-PARLAMENT són de 2.048 bits.

6.1.6. Generació de paràmetres de clau pública

Sense estipulació addicional.

6.1.7. Comprovació de la qualitat dels paràmetres de clau pública

Es realitza d'acord amb la norma ETSI TS 102 176, que indica la qualitat dels algorismes de signatura electrònica.

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

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

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

L'EC-PARLAMENT o l'Entitat de Registre comprova l'autenticitat i el nivell de seguretat de les targetes o dispositius criptogràfics adquirits als proveïdors, abans d'autoritzar-ne l'ús.

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

6.1.9. Propòsits d'ús de claus

L'EC-PARLAMENT inclou l'extensió *KeyUsage* en 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-PARLAMENT) es protegeixen utilitzant maquinari criptogràfic que compleix els requisits establerts per l'especificació tècnica FIPS 140-2 Nivell 3 o superior.

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

6.2.1.2. Cicle de vida de les targetes amb circuit integrat

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

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 part de més d'una persona (n de m) sobre la clau privada

L'accés a les claus privades de l' EC-PARLAMENT requereix la concurrència de, mínim dos (2) dispositius criptogràfics de forma simultània dels cinc (5) possibles actualment existents.

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

6.2.3. Dipòsit de la clau privada

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

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

6.2.4. Còpia de seguretat de la clau privada

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

6.2.5. Arxiu de la clau privada

La clau privada de l'EC-PARLAMENT compta amb una còpia de seguretat realitzada, emmagatzemat, i recuperat en el seu cas per personal subjecte a la política de confiança del personal. Aquest personal està expressament autoritzat per a aquestes finalitats, i es limita a aquell que estrictament requereixin les pràctiques de l'EC-PARLAMENT.

Els controls de seguretat a aplicar en backups de l'EC-PARLAMENT són d'igual o superior nivell als que s'apliquen a les claus habitualment en ús.

Quan les claus s'emmagatzemin en un mòdul hardware de procés dedicat, es preveuen els controls oportuns per a que aquestes no puguin mai abandonar el dispositiu.

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

6.2.6. Introducció de la clau privada en el mòdul criptogràfic

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

Aquestes targetes són utilitzades per a 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 als mòduls criptogràfics.

6.2.8. Mètode d'activació de la clau privada

Es requereixen al menys dos persones per a activar la clau privada de l'EC-PARLAMENT.

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

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 forma que s'impedeix el seu robatori, modificació, divulgació o ús no autoritzat.

6.2.11. Classificació dels mòduls criptogràfics

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

Els mòduls dels subscriptors de certificats de signatura electrònica reconeguda i de certificats de nivell alt obtenen o superen el nivell EAL 4 de Common Criteria (ISO 15408) o FIPS 140-2 nivell 3 amb els augments que determinen a l'especificació tècnica CEN CWA 14169 o equivalent.

6.3. Altres aspectes de gestió del parell de claus

6.3.1. Arxiu de la clau pública

L'EC-PARLAMENT arxiva les seves claus públiques, d'acord amb allò establert a la secció 5.5.

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

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

Com a excepció, la clau privada de desxifrat es pot continuar utilitzant fins a 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-PARLAMENT facilita al subscriptor, per un costat, les dades d'activació de la targeta i, passats 3 dies, 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 distribuir els elements dels certificats per dos canals diferents.

- En primer lloc, el responsable de l'Entitat de Registre lliura al posseïdor de claus el següent material:
 - Full de lliurament de posseïdor
 - Targeta amb els certificats
 - Programari necessari per utilitzar la targeta
 - Carta de lliurament de certificats.

- Al mateix temps, i per correu electrònic, s'envien al posseïdor de claus les dades d'activació del certificat.

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

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

La distribució de les dades d'activació per als certificats de dispositiu CDS-1, CDS-1 EV, CDSCD-1, CDS-1 Seu electrònica de nivell mig EV i CDA-1 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 està limitat a individus degudament autoritzats. En particular:

- L'EC-PARLAMENT garanteix una administració efectiva del nivell d'accés dels usuaris (operadors, administradors, així com de qualsevol usuari amb accés directe al sistema) per a mantenir la seguretat del sistema, incloent-hi la gestió de comptes d'usuari, auditoria i modificacions o denegacions d'accés oportunes.
- L'EC-PARLAMENT garanteix que l'accés als sistemes d'informació i aplicacions es restringeix d'acord amb allò establert a la política de control d'accés, així com que els sistemes proporcionen els controls de seguretat suficients per a implementar la segregació de funcions identificada a les pràctiques de l'EC-PARLAMENT, 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-PARLAMENT està identificat i reconegut abans d'utilitzar aplicacions crítiques relacionades amb el cicle de vida del certificat.
- El personal de l'EC-PARLAMENT és responsable i ha de poder justificar les seves activitats, per exemple mitjançant un arxiu d'esdeveniments.
- S'ha d'evitar la possibilitat de revelació de dades sensibles mitjançant la reutilització d'objectes d'emmagatzematge (per exemple fitxers esborrats) que queden accessibles a usuaris no autoritzats.
- Els sistemes de seguretat i monitorització permeten una ràpida detecció, registre i actuació davant intents d'accés irregulars o no autoritzats als seus recursos (per exemple, mitjançant un sistema de detecció d'intrusions, monitorització i alarma).
- L'accés als Dipòsits públics de la informació de l'EC-PARLAMENT (per exemple, certificats o informació d'estat de revocació) compta amb un control d'accessos per a modificacions o esborrat 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, s'avalua el grau de compliment mitjançant 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 utilitzada en les aplicacions d'Autoritat (tècnica) de Certificació i d'Autoritat (tècnica) de Registre, per a garantir que els sistemes són segurs.

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

6.6.2. Controls de gestió de seguretat

L'EC-PARLAMENT 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-PARLAMENT 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 efectuat.

La configuració dels sistemes s'audita de forma periòdica, d'acord amb allò establert a la secció 8.1 de la present DPC.

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

6.6.3. Avaluació del nivell de seguretat del cicle de vida

Sense estipulació addicional.

6.7. Controls de seguretat de xarxa

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

- S'implementen controls (com per exemple tallafocs) per a protegir la xarxa interna de dominis externs accessibles per terceres parts. Els tallafocs es configuren de forma que s'impedeixen accessos i protocols que no siguin necessaris per a l'operació de l'EC-PARLAMENT.
- Les dades sensibles es protegeixen quan s'intercanvien a través de xarxes no segures (incloent-hi les dades de registre del subscriptor).
- Es garanteix que els components locals de xarxa (com a 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-PARLAMENT realitza periòdicament una auditoria de conformitat per a provar que compleix amb els requisits de seguretat i d'operació necessaris per a formar part de la jerarquia pública de certificació de Catalunya.

L'EC-PARLAMENT pot delegar l'execució de les auditories a favor de CATCert o d'una tercera entitat contractada per CATCert. En aquest cas l'EC-PARLAMENT coopera plenament amb el personal que duu a terme la investigació.

8.1. Frequència de l'auditoria de conformitat

L'EC-PARLAMENT duu 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 s'encarregarà, a través del seu departament d'auditoria o d'un auditor independent i extern amb provada experiència i capacitat, de realitzar l'auditoria de conformitat.

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-PARLAMENT auditada. En cas d'auditoria interna, l'EC-PARLAMENT 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 seran els següents:

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

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

Una vegada s'hagi rebut l'informe de l'auditoria de compliment duta a terme, l'EC-PARLAMENT discuteix amb l'Entitat auditora i amb CATCert, les deficiències detectades i desenvolupa i executa un pla correctiu que soluciona dites deficiències.

Si l'EC-PARLAMENT és incapaç de desenvolupar i/o executar dit pla o si les deficiències trobades suposen una amenaça immediata per a la seguretat o integritat del sistema s'ha de realitzar una de les següents accions:

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

8.6. Tractament dels informes d'auditoria

L'EC-PARLAMENT entrega 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-PARLAMENT, en la prestació dels seus serveis. Les tarifes es poden consultar al web de CATCert (<http://www.catcert.cat/tarifes/>).

9.1.2. Tarifa d'accés a certificats

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

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

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

9.1.4. Tarifes d'altres serveis

Sense estipulació addicional

9.1.5. Política de reintegrament

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

9.2. Capacitat financera

9.2.1. Assegurança de responsabilitat civil

CATCert disposa d'una garantia de cobertura de la seva responsabilitat civil suficient, en els termes previstos a l'article 20.2 de la Llei 59/2003, de 19 de desembre. Aquesta assegurança cobreix les actuacions de CATCert com a prestador de serveis de certificació.

9.2.2. Altres actius

Sense estipulació addicional.

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

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

9.3. Confidencialitat

9.3.1. Informacions confidencials

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

- Informació de negoci subministrada pels seus proveïdors i d'altres persones amb les que CATCert o l'EC-PARLAMENT tenen una obligació de guardar secret, establerta legalment o convencional.
- Registres de transaccions, incloent-hi 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-PARLAMENT i els seus auditors.
- d. Plans de continuïtat del negoci i d'emergència.
- e. Política i procediments de seguretat.
- f. Documentació d'operacions i resta de plans d'operació, tals com l'arxiu, monitorització i d'altres anàlegs.
- g. Qualsevol altra informació identificada com a "Confidencial".

9.3.2. Informacions no confidencials

Les següents informacions no tenen caràcter confidencial:

- a. La Declaració de Pràctiques de Certificació de l'EC-PARLAMENT
- b. Qualsevol altra informació identificada com a "Pública"

9.3.3. Responsabilitat per la protecció d'informació confidencial

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

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

9.4. Protecció de dades personals

9.4.1. Política de Protecció de Dades Personals

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

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

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

SUBSCRIPTORS DE CERTIFICATS:

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

PERSONES FÍSQUES CERTIFICADES:

- Dades identificatives: nom, cognoms i DNI o equivalent de la persona física certificada. Opcionalment, altres dades personals la inclusió de les quals sigui sol·licitada per la persona autoritzada, com el codi CIP de la Targeta Individual Sanitària.

- Dades de contacte: adreça postal completa a efectes de notificacions, així com l'adreça electrònica.
- Dades de l'entitat a la que presten els seus serveis (només en cas de certificats de classe 1 i de classe 2 de col·lectiu).
- Denominació de l'entitat, CIF, àrea d'adscripció política, orgànica, laboral o professional.

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

CATCert desenvolupa els procediments indicats en aquest document, que aplica en la prestació dels seus serveis, en els quals, en compliment dels requisits establerts per les polítiques de certificats que gestiona, i d'acord amb l'article 19 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, es detallen els requisits i obligacions en relació amb l'obtenció i gestió de les dades personals que obtingui, complint a aquest efecte, les disposicions de la Llei Orgànica 15/1999 de 13 de desembre, de Protecció de Dades de Caràcter Personal, i del Reial Decret 1720/2007, de 21 de desembre, que aprova el Reglament de Desenvolupament de la Llei Orgànica 15/1999 de Protecció de Dades de Caràcter Personal (RLOPD).

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

- a. Àmbit d'aplicació del document de seguretat amb especificació detallada dels recursos protegits (article 88 del RD 1720/2007) - secció 9.4
- b. Mesures, normes, procediments, regles i estàndards que garanteixin el nivell de seguretat exigut pel RD 1720/2007 - secció 9.4, i, en general, tots els controls tècnics de les seccions 5 i 6 de la Política General de Certificació de CATCert.
- c. Funcions i obligacions del personal (article 89 del RD 1720/2007) - secció 5.3.
- d. Registre d'incidències (article 90 del RD 1720/2007), procediment de notificació, gestió i resposta davant les incidències – secció 9.4.5
- e. Control d'accés (article 91 del RD 1720/2007) – seccions 5 i 6.
- f. Gestió de suports (article 92 del RD 1720/2007) – secció 5.
- g. Identificació i autenticació (article 93 del RD 1720/2007) – secció 5.2.
- h. Procediments de còpia de seguretat i recuperació de dades (article 94 del RD 1720/2007) - secció 5.5.

9.4.2. Dades de caràcter personal no disponibles a tercers

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

Les dades de caràcter personal que hagin de ser incloses als certificats i al mecanisme indicat de comprovació de l'estat dels certificats són considerades dades de caràcter públic

als efectes de la Llei de Signatura Electrònica. En aquest sentit, no seran considerades dades públiques disponibles a tercers:

- Sol·licituds de certificats, aprovades o denegades, així com tota altra informació personal obtinguda per a l'expedició i manteniment de certificats.
- Claus privades generades i/o emmagatzemades per l'Entitat de Certificació.
- Qualsevol altra dada de caràcter personal que no sigui susceptible de consulta, emmagatzemament o accés per tercers.

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

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

9.4.3. Dades de caràcter personal disponibles a tercers

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

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

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

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

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

9.4.4. Responsabilitat corresponent a la protecció de les dades personals

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

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

CATCert inclou en aquest document el seu procediment de notificació, gestió i resposta davant de les incidències relacionades amb les dades personals.

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

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

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

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

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

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

- El procediment per a la recuperació
- La persona (i autorització) per a la recuperació
- Les dades restaurades.

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

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

En l'expedició de certificats de classe 1, aquestes dades són comunicades pels subscriptors, sense necessitat de consentiment dels afectats posseïdors de claus, d'acord amb l'establert per la normativa reguladora de la relació del personal al servei del subscriptor del certificat o una altra normativa que resulti aplicable, com preveu l'article 6 de la LOPD.

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

9.4.7. Comunicació de dades personals

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

En concret, CATCert està obligada a revelar la identitat dels signants quan ho sol·licitin els òrgans judicials en l'exercici de les funcions que tinguin atribuïdes i en la resta de supòsits previstos a l'article 11.2 de la LOPD.

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

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

9.5. Drets de propietat intel·lectual

9.5.1. Propietat dels certificats i informació de revocació

CATCert és l'única entitat que es beneficia dels drets de propietat intel·lectual sobre els certificats que emeti.

L'EC-PARLAMENT concedeix llicència no exclusiva per a reproduir, distribuir, verificar i utilitzar els certificats, sense cap cost, en relació amb signatures electròniques i/o sistemes de xifrat dintre de l'àmbit d'aplicació de la present DPC, d'acord amb el corresponent instrument vinculant entre l'EC-PARLAMENT i la part que reproduceix i/o distribueix el certificat.

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

Addicionalment, els certificats emesos per l'EC-PARLAMENT contenen un avís legal relatiu a la propietat d'aquests.

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

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

L'EC-PARLAMENT n'és propietària de la present DPC.

9.5.3. Propietat de la informació relativa a noms

El subscriptor i, en el seu cas, el posseïdor de claus conserva qualsevol dret, d'existir aquest, relatiu a la marca, producte o nom comercial contingut en el certificat.

El subscriptor i, en el seu cas, el posseïdor de claus és el propietari del nom distingit del certificat, format per les informacions especificades a la secció 3.1 de la present DPC.

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. EC-PARLAMENT

9.6.1.1. Obligacions generals de l'EC-PARLAMENT

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

- Determina la comunitat de subscriptors i verificadors de l'EC-PARLAMENT.
- 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-PARLAMENT, d'acord amb el procediment previst en aquesta Declaració de Pràctiques de Certificació. i
- Informa puntualment CATCert de totes les informacions relatives als canvis a realitzar, incidències en el servei, reclamacions, denúncies i inspeccions del servei.
- Garanteix sota la seva plena responsabilitat, que compleix amb tots els requisits establerts en aquest document.
- És l'única entitat responsable del compliment dels procediments descrits en aquest document, inclòs quan una part o la totalitat de les operacions siguin subcontractades externament.
- Presta els seus serveis de certificació d'acord amb aquest document on es detallen almenys els continguts previstos a l'article 19 de la Llei 59/2003.

- Abans de l'emissió i lliurament del certificat al subscriptor, l'EC-PARLAMENT l'informa dels aspectes previstos a l'article 18. b) de la Llei 59/2003, i dels següents aspectes:
 - Indicació de la política aplicable, amb indicació de si els certificats s'expedeixen al públic i de la necessitat d'utilització de dispositiu segur de creació de signatura.
 - Forma en que es garanteix la responsabilitat patrimonial per part de l'EC-PARLAMENT.
 - L'EC-PARLAMENT declara que té la certificació del prestador de serveis de certificació i la certificació dels productes de signatura electrònica utilitzats.
- Aquest requisit es compleix mitjançant un "Text divulgatiu de la política de certificat" aplicable, que es transmet electrònicament, utilitzant un mitjà de comunicació durador en el temps, i en llenguatge comprensible.
- Obliga els subscriptors, els posseïdors de claus i els verificadors mitjançant instruments jurídics apropiats a cada situació
- Aquests instruments jurídics es transmeten electrònicament, estant en llenguatge escrit i comprensible, i tenint els següents continguts mínims:
 - Prescripcions per donar compliment a l'establert en aquest document.
 - Indicació de la política aplicable, amb indicació de si els certificats s'expedeixen al públic i de la necessitat d'ús del dispositiu segur de creació de signatura.
 - Manifestació que la informació continguda al certificat és correcta, excepte notificació en contra pel subscriptor.
 - Consentiment per a la publicació del certificat en el directori i accés per tercers al mateix.
 - Consentiment per a l'emmagatzematge de la informació utilitzada per al registre del subscriptor i del posseïdor de claus, per a la provisió del dispositiu segur de creació de signatura i per a la cessió de la informació esmentada en tercers, en cas de final d'operacions de l'EC-PARLAMENT sense revocació de certificats vàlids.
 - Límits d'ús del certificat, incloent els establerts a la secció 4.5 d'aquest document.
 - Informació sobre com validar un certificat, incloent el requisit de comprovar l'estat del certificat, i les condicions en les quals es pot confiar raonablement en el certificat, que resulta aplicable quan el subscriptor actua com a verificador.
 - Limitacions de responsabilitat aplicables, incloent els usos pels quals l'EC-PARLAMENT accepta o exclou la seva responsabilitat.
 - Procediments aplicables de resolució de disputes.
 - Llei aplicable i jurisdicció competent.
- L'EC-PARLAMENT 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-PARLAMENT 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 a l'article 13 de la Llei 59/2003, de signatura electrònica
- Quan el subscriptor del certificat de persona física és una persona jurídica, l'EC-PARLAMENT comprova que el posseïdor de claus es troba degudament autoritzat pel subscriptor.
- L'EC-PARLAMENT, com a Entitat de Certificació Virtual, s'obliga al següent:
 - Determinar la comunitat de subscriptors i verificadors
 - Aprovar les polítiques de certificació i, si és necessari, las polítiques específiques de certificació.
 - Aprovar la Declaració de Pràctiques de Certificació.
 - Aprovar la documentació contractual i reguladora dels serveis de certificació en la comunitat d'usuaris.
 - Notificar puntualment a CATCert totes les informacions relatives als canvis a realitzar, incidències en els serveis, reclamacions, denúncies i inspeccions del servei.

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

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

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

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

9.6.1.3. Informació per als certificats personals

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

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

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

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

9.6.1.4. Garanties ofertes a subscriptors i a verificadors

L'EC-PARLAMENT, com a mínim, garanteix al subscriptor, i 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.
- f. Que el certificat conté les informacions que ha de contenir un certificat reconegut, d'acord amb l'article 11.2 de la Llei 59/2003, de 19 de desembre
- g. Que, en el cas que generi les claus privades del subscriptor o, en el seu cas, del posseïdor de claus, es manté la seva confidencialitat durant el procés.
- h. La responsabilitat de l'EC-PARLAMENT, amb els límits que s'estableixin.

9.6.2. Obligaciones y otros compromisos de las Entidades de Registro

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

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

L'EC-PARLAMENT, d'acord amb aquest document, i la documentació d'operacions de l'EC-PARLAMENT.

- g. Emmagatzema els registres, ja sigui en paper, ja sigui de forma electrònica, amb les adequades mesures de seguretat, autenticitat, integritat i conservació, relatius a la informació continguda al certificat, durant un període de 15 anys. Aquests registres estan a disposició de l'EC-PARLAMENT.
- h. Aporta la justificació documental necessària per al registre d'usuaris i per a la posterior emissió de certificats per part de l'EC-PARLAMENT o l'Entitat de Registre.
- i. La justificació documental es realitza per una unitat orgànica de l'Entitat de Registre facultada legalment per donar fe de les dades a certificar, que s'indiquen a CATCert.

9.6.2.2 Garanties ofertes a subscriptor i verificadors

9.6.2.2.1 Garantia de CATCert pels serveis de certificació digital

CATCert garanteix que la clau privada de l'EC-PARLAMENT utilitzada per emetre certificats no ha estat compromesa, excepte que CATCert no hagués comunicat el contrari mitjançant el Dipòsit de CATCert.

CATCert únicament garanteix que:

- a) Els certificats de signatura electrònica contenen tota la informació exigida per la Llei 59/2003, de 19 de desembre.
- b) 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, d'arxiu i de seguretat descrits en aquest document i el conveni de referència.

9.6.2.2.2 Exclusió de la garantia

CATCert no garanteix cap software utilitzat pel subscriptor o per qualsevol altra persona, per a generar, verificar o utilitzar de forma diferent, signatura electrònica alguna o certificat digital emès per CATCert, excepte els 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. Requisits per a tots els tipus de certificats

L'EC-PARLAMENT obliga al subscriptor a:

- a. Facilitar a l'EC-PARLAMENT informació completa i adequada, conforme als requeriments d'aquesta política de certificació, en especial en allò relatiu 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 la present DPC i a l'article 23.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.
- d. Utilitzar el certificat d'acord amb allò establert a la secció 1.4 de la present DPC.
- e. Notificar a l'EC-PARLAMENT, sense endarreriments injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu segur de creació de signatura.
- f. Notificar a l'EC-PARLAMENT i a qualsevol altra persona que el subscriptor cregui que pot confiar en el certificat, sense endarreriments injustificables:
 - a La pèrdua, el robatori o el compromís potencial de la seva clau privada.
 - b La pèrdua de control sobre la seva clau privada, a causa del compromís de les dades d'activació (per exemple, el codi PIN del dispositiu segur de creació de signatura) o per qualsevol altra causa.
 - c Les inexactituds o canvis en el contingut del certificat que conegui o pugui conèixer el subscriptor.
- g. Deixar d'utilitzar la clau privada una vegada transcorregut el període indicat a la secció corresponent.
- h. Transferir als posseïdors de claus les obligacions específiques d'aquests.
- i. 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.
- j. 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-PARLAMENT obliga al subscriptor a:

- a. Utilitzar el parell de claus exclusivament per a signatures electròniques i conforme a qualsevol altra limitació que li hagi estat notificada.
- b. Reconèixer que aquestes signatures electròniques són signatures electròniques equivalents a signatures manuscrites, d'acord amb l'article 3.4 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.
- c. Ser especialment diligent en la custòdia de la seva clau privada i del seu dispositiu segur de creació de signatura, a fi i efecte d'evitar usos no autoritzats.
- d. Notificar a l'EC-PARLAMENT, 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:

- a. Generar les seves claus de subscriptor utilitzant un algoritme reconegut com a acceptable per a la signatura electrònica reconeguda.
- b. Crear les claus dintre del dispositiu segur de creació de signatura.
- c. Utilitzar longituds i algoritmes de clau reconeguts com a acceptables per a la signatura electrònica reconeguda.

9.6.3.2. Garanties oferides pel subscriptor

El subscriptor s'obliga, mitjançant el corresponent instrument jurídic, a garantir:

- a. Que totes les manifestacions realitzades en la sol·licitud són correctes.
- b. Que totes les informacions subministrades pel subscriptor que es troben contingudes en el certificat són correctes.
- c. Que el certificat s'utilitza exclusivament per a usos legals i autoritzats, d'acord amb la present DPC.
- d. Que cada signatura digital creada amb la clau privada corresponent a la clau pública llistada en el 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 en el certificat per a signar cap altre certificat (o qualsevol altre format de clau pública certificada), ni LRC.
- f. Que cap persona no autoritzada ha tingut mai accés a la clau privada del subscriptor.

9.6.3.3. Protecció de la clau privada

L'EC-PARLAMENT obliga al subscriptor, mitjançant el corresponent instrument jurídic, a garantir que 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-PARLAMENT obliga a 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 la qual cosa utilitzarà 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 de que es trobi en el mateix certificat o en el contracte de verificador.
- e. Tenir present qualsevol precaució establerta en un contracte o en altre instrument, amb independència de la seva naturalesa jurídica.

- f. No monitorar, manipular o realitzar actes de enginyeria inversa sobre la implantació tècnica de la jerarquia pública de certificació de Catalunya, sense permís previ per escrit.
- g. No comprometre intencionadament la seguretat de la jerarquia pública de certificació de Catalunya.
- h. Reconèixer que les signatures electròniques produïdes per certificats de signatura electrònica reconeguda, són signatures electròniques equivalents a signatures escrites, d'acord amb l'article 3.4 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

9.6.4.2. Garanties oferides pel verificador

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

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

L'EC-PARLAMENT pot delegar algunes funcions en el directori, que en aquest cas està obligat al seu compliment, en les mateixes condicions que aquesta.

Les funcions, obligacions i deures del directori s'estableixen detalladament a la present DPC, així com a la documentació jurídica auxiliar, especialment la entregada a subscriptors, posseïdors de claus i verificadors.

9.6.5.2. Garanties oferides pel directori

L'EC-PARLAMENT estableix a la present DPC la responsabilitat civil del directori, quan sigui operat per una tercera entitat.

9.7. Renúncies de garanties

9.7.1. Rebuig de garanties de l'EC-PARLAMENT

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

9.8. Limitacions de responsabilitat

9.8.1. Limitacions de responsabilitat de l'EC-PARLAMENT

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

9.8.2. Cas fortuït i força major

L'EC-PARLAMENT inclou clàusules per a limitar la seva responsabilitat en supòsits de cas fortuït i de força major, en els instruments jurídics amb els que vinculi subscriptors i verificadors.

9.9. Indemnitzacions

9.9.1. Clàusula d'indemnitat de subscriptor

No s'establirà clàusula d'indemnitat del subscriptor.

9.9.2. Clàusula d'indemnitat de verificador

No s'establirà clàusula d'indemnitat del verificador.

9.10. Termini i finalització

9.10.1. Termini

L'EC-PARLAMENT estableix, en els 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 es subministren certificats als subscriptors.

9.10.2. Finalització

L'EC-PARLAMENT estableix, en els seus instruments jurídics amb els subscriptors i els verificadors, una clàusula que determina les conseqüències de la finalització de la relació jurídica en virtut de la qual se subministren certificats als subscriptors.

9.10.3. Supervivència

CATCert determinarà un Pla de Continuïtat de Negoci. Aquest Pla de Continuïtat de Negoci determinarà 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 aquest 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.

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

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

9.11. Notificacions

L'EC-PARLAMENT estableix, en els seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules de notificació.

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

9.12. Modificacions

9.12.1. Procediment per a les modificacions

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

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

9.12.2. Termini i mecanismes per a notificacions

Les modificacions de la present DPC es notifiquen a CATCert, per a la seva posterior aprovació.

9.12.3. Circumstàncies en les que un OID ha de ser canviat

Sense estipulació addicional.

9.13. Resolució de conflictes

9.13.1. Resolució extrajudicial de conflictes

L'EC-PARLAMENT estableix, en els 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-PARLAMENT.

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

9.13.2. Jurisdicció competent

L'EC-PARLAMENT estableix, en els 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 en resulten d'aplicació.

Tanmateix, es té en compte la legislació administrativa que resulti aplicable.

9.14. Llei aplicable

L'EC-PARLAMENT estableix, en els 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-PARLAMENT 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-PARLAMENT manifesta el compliment de la Llei 59/2003, de 19 de desembre, de signatura electrònica, en la present DPC.

9.16. Clàusules diverses

9.16.1. Acord íntegre

L'EC-PARLAMENT estableix, en els 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 de Entitat de Certificació no poden ser objecte de cessió a tercers de cap tipus, ni cap tercera entitat es pot subrogar en la posició jurídica d'una Entitat de Certificació.

En cas de produir-se una cessió o subrogació, es procedeix a la finalització de l'EC-PARLAMENT.

9.16.3. Divisibilitat

L'EC-PARLAMENT estableix en 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 a la resta del contracte.

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

9.16.4. Aplicacions

Sense estipulació addicional.

9.16.5. Altres clàusules

Sense estipulació addicional.

2.

Annex I.

Projecte:	Informe modificació del document DPC EC-Parlament
Entitat de destí:	Agència Catalana de Certificació
Codi de referència:	Revisió 2n semestre 2010
Versió:	Canvis de la v1.5 a la v 1.6 en català i en castellà
Data de l'edició:	30/06/2011

Control de versions DPC EC-Parlament 1r semestre 2011

Versió	Parts que canvien	Descripció del canvi	Autor del canvi	Data del canvi
3.7	1.1.1.2, 1.1.1.4, 1.2.2, 6.1	Introducció CPIXSA Càrrec EP, CDS-1 EV i característiques CDS-1 Seu electrònica EV (nivell mig i alt)	Oficina de Polítiques	30/06/2011
3.7	4.4.1.1	Adaptació del procediment de lliurament al refactoring	Oficina de Polítiques	30/06/2011
3.7	4.9.1.6	Inclusió de causa de revocació per als CDP	Oficina de Polítiques	30/06/2011
3.7	5.8.1	Modificació de les condicions per a l'acabament del servei	Oficina de Polítiques	30/06/2011
3.7	6.1.5	Adaptació mides claus	Oficina de Polítiques	30/06/2011

3.7	6.4.2	Adaptació del procediment de lliurament de les dades d'activació al procediment (refactoring)	Oficina de Polítiques	30/06/2011
3.7	5.8.2	Custòdia de documentació per les Entitats de Registre	Oficina de Polítiques	30/06/2011
3.7	9.6	Reestructuració de la informació relativa a les obligacions de l'EC i les ER	Oficina de Polítiques	30/06/2011