



**Agència Catalana  
de Certificació**

---

**Declaració de Pràctiques de Certificació**  
**Entitat de Certificació Agència Catalana de Certificació**


---

**(EC-ACC)**

Referència: D1111\_E0650\_N-DPC EC-ACC  
Versió: 1.2  
Data: 30/06/2011

---

## Control documental

<b>Estat formal</b>	<b>Elaborat per:</b>  Carlos Alonso – Núria Mombiola (Àrea d'Assessorament)	<b>Aprovat per:</b>  Marta Cruellas
<b>Data de creació</b>	26/09/2006	
<b>Control de versions</b>	<b>Data:</b>	
	<b>Descripció:</b>	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.)
<b>Nivell accés informació</b>	pública	
<b>Títol</b>	Declaració de Pràctiques de Certificació EC-ACC v1r2 cat	
<b>Fitxer</b>	D1111 E0650 N-DPC EC-ACC v1r2 cat.pdf	
<b>Control de còpies</b>	Només les còpies disponibles a <a href="https://www.catcert.cat/">https://www.catcert.cat/</a> garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.	
<b>Drets d'autor</b>	 <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 <a href="http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca">http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca</a> o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.</p>	

## Índex

<b>Índex.....</b>	<b>3</b>
<b>1. Introducció.....</b>	<b>11</b>
1.1 PRESENTACIÓ .....	11
1.1.1 Tipus i classes de certificats .....	12
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 .....	19
1.3.2 Entitat de Certificació Arrel .....	20
1.3.3 Entitats de Certificació Vinculades.....	20
1.3.4 Entitats de Registre .....	20
1.3.5 Usuaris finals.....	20
1.4 ÚS DELS CERTIFICATS.....	22
1.4.1 Usos típics dels certificats .....	22
1.4.2 Aplicacions prohibides.....	25
1.5 ADMINISTRACIÓ DE LA DECLARACIÓ DE PRÀCTIQUES .....	25
1.5.1 Organització que administra l'especificació .....	25
1.5.2 Dades de contacte de l'organització .....	26
1.5.3 Persona que determina la conformitat de la Declaració de Pràctiques de Certificació (DPC) amb la política .....	26
1.5.4 Procediment d'aprovació .....	26
<b>2. Publicació d'informació i directori de certificats .....</b>	<b>27</b>
2.1 DIRECTORI DE CERTIFICATS .....	27
2.2 PUBLICACIÓ D'INFORMACIÓ DE L'EC-ACC.....	27
2.3 FREQUÈNCIA DE PUBLICACIÓ .....	27
2.4 CONTROL D'ACCÉS .....	28
<b>3. Identificació i autenticació.....</b>	<b>29</b>
3.1 GESTIÓ DE NOMS .....	29
3.1.1 Tipus de noms.....	29
3.1.2 Significat dels noms .....	29
3.1.3 Utilització d'anònims i pseudònims .....	29
3.1.4 Interpretació de formats de noms .....	29

3.1.5	Unicitat dels noms .....	29
3.1.6	Resolució de conflictes relatius a noms .....	30
3.2	VALIDACIÓ INICIAL DE LA IDENTITAT .....	31
3.2.1	Prova de possessió de clau privada .....	31
3.2.2	Autenticació de la identitat d'una Organització .....	31
3.2.3	Autenticació de la identitat d'una persona física .....	32
3.2.4	Informació no verificada .....	33
3.3	IDENTIFICACIÓ I AUTENTICACIÓ DE SOL·LICITUDS DE RENOVACIÓ .....	33
3.3.1	Validació per a la renovació rutinària de certificats .....	33
3.3.2	Validació per a la renovació de certificats després de la revocació.....	33
3.4	IDENTIFICACIÓ I AUTENTICACIÓ DE LA SOL·LICITUD DE REVOCACIÓ .....	33
3.5	AUTENTICACIÓ D'UNA PETICIÓ DE SUSPENSIO .....	33
<b>4.</b>	<b>Característiques d'operació del cicle de vida dels certificats .....</b>	<b>34</b>
4.1	SOL·LICITUD D'EMISSIÓ DE CERTIFICAT .....	34
4.1.1	Legitimació per sol·licitar l'emissió .....	34
4.1.2	Procediment d'alta; Responsabilitats .....	34
4.2	PROCESSAMENT DE LA SOL·LICITUD DE CERTIFICACIÓ .....	34
4.2.1	Requisits per a tot tipus de certificats .....	34
4.2.2	Requisits addicionals per al Certificat CIC .....	35
4.3	EMISSIÓ DE CERTIFICAT .....	35
4.3.1	Accions de l'EC-ACC durant el procés d'emissió.....	35
4.3.2	Notificació de l'emissió al subscriptor .....	36
4.4	ACCEPTACIÓ DEL CERTIFICAT .....	36
4.4.1	Responsabilitats del Prestador de Serveis de Certificació .....	36
4.4.2	Conducta que constitueix acceptació del certificat.....	37
4.4.3	Publicació del certificat .....	37
4.4.4	Notificació de l'emissió a tercers .....	37
4.5	ÚS DEL PARELL DE CLAUS I DEL CERTIFICAT .....	37
4.5.1	Ús pels posseïdors de claus .....	37
4.5.2	Ús pel tercer que confia en certificats .....	38
4.6	RENOVACIÓ DE CERTIFICATS SENSE RENOVACIÓ DE CLAUS .....	38
4.7	RENOVACIÓ DE CERTIFICATS AMB RENOVACIÓ DE CLAUS.....	38
4.8	MODIFICACIÓ DE CERTIFICATS .....	38
4.9	REVOCACIÓ I SUSPENSIO DE CERTIFICATS.....	39
4.9.1	Causes de revocació de certificats .....	39
4.9.2	Legitimació per sol·licitar la revocació .....	40

4.9.3	Procediments de sol·licitud de revocació .....	40
4.9.4	Període temporal de sol·licitud de revocació .....	41
4.9.5	Període màxim de processament de la sol·licitud de revocació .....	41
4.9.6	Obligació de consulta d'informació de revocació de certificats .....	41
4.9.7	Freqüència d'emissió de llistes de revocació de certificats (LRCs) .....	41
4.9.8	Període màxim de publicació de LRCs .....	41
4.9.9	Disponibilitat de serveis de comprovació d'estat de certificats .....	42
4.9.10	Obligació de consulta de serveis de comprovació d'estat de certificats .....	42
4.9.11	Altres formes d'informació de revocació de certificats .....	42
4.9.12	Procediments especials en cas de compromís de la clau privada .....	42
4.9.13	Causas de suspensió de certificats .....	43
4.9.14	Qui pot sol·licitar la suspensió .....	43
4.9.15	Procediments de petició de suspensió .....	43
4.9.16	Període màxim de suspensió .....	44
4.9.17	Habilitació d'un certificat suspès .....	44
4.10	SERVEIS DE COMPROVACIÓ D'ESTAT DE CERTIFICATS .....	44
4.10.1	Característiques d'operació dels serveis .....	44
4.10.2	Disponibilitat dels serveis .....	44
4.10.3	Altres funcions dels serveis .....	45
4.11	FINALITZACIÓ DE LA SUBSCRIPCIÓ .....	45
4.12	DIPÒSIT I RECUPERACIÓ DE CLAUS .....	45
4.12.1	Política i pràctiques de dipòsit i recuperació de claus .....	45
4.12.2	Política i pràctiques d'encapçalament i recuperació de claus de sessió .....	45
<b>5.</b>	<b>Controls de seguretat física, de gestió i d'operacions .....</b>	<b>46</b>
5.1	CONTROLS DE SEGURETAT FÍSICA .....	46
5.1.1	Àrees segures .....	46
5.1.2	Controls de seguretat física .....	46
5.1.3	Localització i construcció de les instal·lacions .....	47
5.1.4	Accés físic .....	47
5.1.5	Electricitat i aire condicionat .....	47
5.1.6	Exposició a l'aigua .....	48
5.1.7	Advertència i protecció d'incendis .....	48
5.1.8	Emmagatzematge de suports .....	48
5.1.9	Tractament de residus .....	48
5.1.10	Còpia de seguretat fora de les instal·lacions .....	48

5.2	CONTROLS DE PROCEDIMENTS .....	48
5.2.1	Funcions fiables .....	49
5.2.2	Nombre de persones per tasca .....	49
5.2.3	Identificació i autenticació per a cada funció.....	49
5.2.4	Rols que requereixen separació de tasques.....	49
5.3	CONTROLS DE PERSONAL .....	50
5.3.1	Requisits d'historial, qualificacions, experiència i autorització.....	51
5.3.2	Requisits de formació .....	51
5.3.3	Requisits i freqüència d'actualització formativa.....	52
5.3.4	Seqüència i freqüència de rotació laboral.....	52
5.3.5	Sancions per accions no autoritzades .....	52
5.3.6	Requisits de contractació de professionals.....	52
5.3.7	Subministrament de documentació al personal .....	52
5.4	PROCEDIMENTS D'AUDITORIA DE SEGURETAT .....	52
5.4.1	Tipus d'esdeveniments registrats .....	52
5.4.2	Freqüència de tractament de registres d'auditoria .....	53
5.4.3	Període de conservació de registres d'auditoria .....	53
5.4.4	Protecció dels registres d'auditoria .....	54
5.4.5	Procediments de còpia de seguretat .....	54
5.4.6	Localització del sistema d'acumulació de registres d'auditoria .....	54
5.4.7	Notificació de l'esdeveniment d'auditoria al causant de l'esdeveniment .....	54
5.4.8	Anàlisi de vulnerabilitats .....	54
5.5	ARXIU D'INFORMACIONS.....	55
5.5.1	Tipus d'esdeveniments registrats .....	55
5.5.2	Període de conservació de registres .....	55
5.5.3	Protecció de l'arxiu .....	55
5.5.4	Procediments de còpia de seguretat .....	56
5.5.5	Requisits de segellat de cautela de data i hora .....	56
5.5.6	Localització del sistema d'arxiu .....	56
5.5.7	Procediments d'obtenció i verificació d'informació d'arxiu .....	56
5.6	RENOVACIÓ DE CLAUS .....	56
5.7	COMPROMÍS DE CLAUS I RECUPERACIÓ DE DESASTRE .....	56
5.7.1	Procediment de gestió d'incidències i compromisos.....	56
5.7.2	Corrupció de recursos, aplicacions o dades .....	56
5.7.3	Compromís de la clau privada de l'Entitat.....	56

5.7.4	Desastre sobre les instal·lacions .....	57
5.8	FINALITZACIÓ DEL SERVEI .....	57
5.8.1	EC-ACC .....	57
5.8.2	Entitat de Registre .....	58
<b>6.</b>	<b>Controls de seguretat tècnica .....</b>	<b>59</b>
6.1	GENERACIÓ I INSTAL·LACIÓ DEL PARELL DE CLAUS .....	59
6.1.1	Generació del parell de claus .....	59
6.1.2	Enviament de la clau privada al subscriptor .....	59
6.1.3	Enviament de la clau pública a l'emissor del certificat .....	59
6.1.4	Distribució de la clau pública del Prestador de Serveis de Certificació .....	59
6.1.5	Mesures de claus .....	60
6.1.6	Generació de paràmetres de clau pública .....	60
6.1.7	Comprovació de qualitat de paràmetres de clau pública .....	60
6.1.8	Generació de claus en aplicacions informàtiques o en béns d'equip .....	60
6.1.9	Propòsits d'ús de claus .....	60
6.2	PROTECCIÓ DE LA CLAU PRIVADA .....	60
6.2.1	Estàndards de mòduls criptogràfics .....	60
6.2.2	Control per més d'una persona (n de m) sobre la clau privada .....	61
6.2.3	Dipòsit de la clau privada .....	61
6.2.4	Còpia de seguretat de la clau privada .....	61
6.2.5	Arxiu de la clau privada .....	61
6.2.6	Introducció de la clau privada en el mòdul criptogràfic .....	62
6.2.7	Emmagatzematge de la clau privada en el mòdul criptogràfic .....	62
6.2.8	Mètode d'activació de la clau privada .....	62
6.2.9	Mètode de desactivació de la clau privada .....	62
6.2.10	Mètode de destrucció de la clau privada .....	62
6.2.11	Classificació dels mòduls criptogràfics .....	62
6.3	ALTRES ASPECTES DE GESTIÓ DEL PARELL DE CLAUS .....	62
6.3.1	Arxiu de la clau pública .....	62
6.3.2	Períodes d'utilització de les claus pública i privada .....	62
6.4	DADES D'ACTIVACIÓ .....	63
6.4.1	Generació i instal·lació de les dades d'activació .....	63
6.4.2	Protecció de dades d'activació .....	63
6.4.3	Altres aspectes de les dades d'activació .....	63
6.5	CONTROLS DE SEGURETAT INFORMÀTICA .....	63

6.5.1	Requisits tècnics específics de seguretat informàtica .....	63
6.5.2	Avaluació del nivell de seguretat informàtica .....	64
6.6	CONTROLS TÈCNICS DEL CICLE DE VIDA .....	64
6.6.1	Controls de desenvolupament de sistemes .....	64
6.6.2	Controls de gestió de seguretat .....	64
6.6.3	Avaluació del nivell de seguretat del cicle de vida .....	65
6.7	CONTROLS DE SEGURETAT DE XARXA.....	65
6.8	SEGELL DE TEMPS.....	65
<b>7.</b>	<b>Perfils de certificats i llistes de certificats revocats .....</b>	<b>66</b>
7.1	PERFIL DE CERTIFICAT .....	66
7.2	PERFIL DE LA LLISTA DE REVOCACIÓ DE CERTIFICATS.....	66
<b>8.</b>	<b>Auditoria de conformitat .....</b>	<b>67</b>
8.1	FREQÜÈNCIA DE L' AUDITORIA DE CONFORMITAT .....	67
8.2	IDENTIFICACIÓ I QUALIFICACIÓ DE L' AUDITOR.....	67
8.3	RELACIÓ DE L' AUDITOR AMB L' ENTITAT AUDITADA .....	67
8.4	RELACIÓ D' ELEMENTS OBJECTE D' AUDITORIA .....	67
8.5	ACCIONS A EMPRENDRE COM A RESULTAT D' UNA MANCA DE CONFORMITAT .....	68
8.6	TRACTAMENT DELS INFORMES D' AUDITORIA .....	68
<b>9.</b>	<b>Requisits comercials i legals.....</b>	<b>69</b>
9.1	TARIFES .....	69
9.1.1	Tarifa d'emissió o renovació de certificats .....	69
9.1.2	Tarifa d'accés a certificats .....	69
9.1.3	Tarifa d'accés a informació d'estat de certificat .....	69
9.1.4	Tarifes d'altres serveis.....	69
9.1.5	Política de reintegrament.....	69
9.2	CAPACITAT FINANCERA.....	69
9.2.1	Assegurança de responsabilitat civil.....	69
9.2.2	Altres actius.....	69
9.2.3	Cobertura d'assegurament per a subscriptors i tercers que confiïn en certificats .....	70
9.3	CONFIDENCIALITAT .....	70
9.3.1	Informacions confidencials .....	70
9.3.2	Informacions no confidencials .....	70
9.3.3	Responsabilitat per a la protecció d'informació confidencial .....	70
9.4	PROTECCIÓ DE DADES PERSONALS .....	71
9.4.1.	Política de Protecció de Dades Personals .....	71
9.4.2.	Dades de caràcter personal no disponibles a tercers .....	72
9.4.3.	Dades de caràcter personal disponibles a tercers .....	72



9.4.4.	Responsabilitat corresponent a la protecció de les dades personals .....	73
9.4.5.	Gestió d'incidències relacionades amb les dades de caràcter personal .....	73
9.4.6.	Prestació del consentiment per al tractament de les dades personals .....	74
9.4.7.	Comunicació de dades personals .....	74
9.5	DRETS DE PROPIETAT INTEL·LECTUAL .....	75
9.5.1	Propietat dels certificats i informació de revocació .....	75
9.5.2	Propietat de la política de certificat i Declaració de Pràctiques de Certificació	75
9.5.3	Propietat de la informació relativa a noms .....	75
9.5.4	Propietat de claus .....	75
9.6	OBLIGACIONS I RESPONSABILITAT CIVIL .....	76
9.6.1	EC-ACC .....	76
9.6.2	Entitats de Registre .....	78
9.6.3	Subscriptors .....	79
9.6.4	Verificadors .....	80
9.6.5	CATCert .....	81
9.6.6	Directori .....	82
9.7	RENÚNCIES DE GARANTIES .....	82
9.7.1	Rebuig de garanties de l'EC-ACC .....	82
9.8	LIMITACIONS DE RESPONSABILITAT .....	83
9.8.1	Limitacions de responsabilitat de l'EC-ACC .....	83
9.8.2	Cas fortuït i força major .....	83
9.9	INDEMNITZACIONS .....	83
9.9.1	Clàusula d'indemnitat de subscriptor .....	83
9.9.2	Clàusula d'indemnitat de verificador .....	83
9.10	TERMINI I FINALITZACIÓ .....	83
9.10.1	Termini .....	83
9.10.2	Finalització .....	83
9.10.3	Supervivència .....	83
9.11	NOTIFICACIONS .....	84
9.12	MODIFICACIONS .....	84
9.12.1	Procediment per a les modificacions .....	84
9.12.2	Període i mecanismes per a notificacions .....	84
9.12.3	Circumstàncies en les quals un OID s'ha de canviar .....	84
9.13	RESOLUCIÓ DE CONFLICTES .....	85
9.13.1	Resolució extrajudicial de conflictes .....	85

9.13.2	Jurisdicció competent .....	85
9.14	LLEI APLICABLE.....	85
9.15	CONFORMITAT AMB LA LLEI APLICABLE.....	85
9.16	CLÀUSULES DIVERSES .....	86
9.16.1	Acord íntegre.....	86
9.16.2	Subrogació .....	86
9.16.3	Divisibilitat .....	86
9.16.4	Aplicacions .....	86
9.16.5	Altres clàusules .....	86
<b>ANNEX I.....</b>		<b>87</b>
CONTROL DOCUMENTAL .....		87
CONTROL DE VERSIONS DPC EC-ACC 1r SEMESTRE 2011 .....		87

## 1. Introducció

Aquest document és la Declaració de Pràctiques de Certificació de l'Entitat de Certificació de l'Agència Catalana de Certificació (d'ara endavant, EC-ACC), Entitat de Certificació Arrel de la jerarquia pública de certificació de Catalunya.

En aquesta DPC es regulen tècnicament i operativament els serveis de certificació de l'EC-ACC.

Els apartats amb el contingut "Sense estipulació addicional" indiquen que s'ha de consultar la Política General de Certificació de CATCert.

### 1.1 Presentació

Quan es va desenvolupar el pacte institucional signat el 23 de juliol del 2001 pels grups parlamentaris del Parlament de Catalunya, la Generalitat de Catalunya i el Consorci d'Ens Locals de Catalunya (Localret), per al desenvolupament de polítiques que permetin afrontar el canvi fonamental en les estructures socials i econòmiques derivat de la confluència de les noves tecnologies de la informació i de la comunicació en l'àmbit de les administracions públiques catalanes, es va decidir establir sistemes d'interrelació entre les esmentades administracions, i entre les administracions i els ciutadans, per via telemàtica i electrònica, en les condicions de seguretat necessàries i, especialment, fent ús de certificats digitals d'identitat i signatura electrònica.

En compliment de l'esmentat pacte institucional i per tal de desenvolupar el programa Catalunya en Xarxa, Localret i la Generalitat de Catalunya van acordar la creació del Consorci per a l'Administració Oberta Electrònica de Catalunya, amb la finalitat de desenvolupar polítiques públiques en matèria de serveis electrònics a les administracions públiques i d'exercir la condició d'autoritat (tècnica) de certificació de signatura electrònica per garantir el secret, la integritat, la identitat i l'autenticitat en les comunicacions i documents electrònics que es produeixen en l'àmbit de les administracions públiques catalanes.

El 25 de febrer del 2002 va tenir lloc la sessió constitutiva del Consorci per a l'Administració Oberta Electrònica de Catalunya, una sessió en la qual el Consell General va adoptar, d'entre altres, l'acord de constituir un ens de gestió directa sota la forma d'organisme autònom de caràcter comercial amb la denominació d'Agència Catalana de Certificació (CATCert) i amb l'objectiu de gestionar certificats digitals i prestar altres serveis relacionats amb la signatura electrònica en l'àmbit públic català.

CATCert es va crear per acord de la Comissió Executiva del Consorci de l'Administració Oberta Electrònica de Catalunya, de 29 d'abril del 2002, com a organisme autònom de caràcter comercial, els estatuts de la qual van ser publicats al Diari Oficial de la Generalitat de Catalunya el 30 de maig del 2003, per Resolució PRE/1574/2003, de 15 de maig.

Per tant, l'Agència Catalana de Certificació es constitueix en l'entitat principal del sistema públic català de certificació que regula l'emissió i la gestió dels certificats que s'emeten per a les institucions d'autogovern de Catalunya, les institucions que integren el món local i la resta d'entitats públiques i privades que integren el sector públic català; així com l'admissió i l'ús dels certificats emesos a ciutadans i empreses per altres prestadors de serveis de certificació i que sol·licitin la corresponent classificació.

Aquestes institucions emetran certificats per mitjà d'una infraestructura tècnica proporcionada per CATCert, denominada "jerarquia pública de certificació de Catalunya", i podran admetre i utilitzar certificats d'altres prestadors mitjançant els serveis de classificació i validació de CATCert.

En aquest sentit, CATCert va crear el 8 de gener del 2003, una jerarquia d'entitats de certificació, l'arrel de la qual és la pròpia Agència.

L'Entitat de certificació de CATCert (denominada EC-ACC) és l'arrel de la jerarquia de confiança, i certifica les Entitats de Certificació que es creen dins del marc de les administracions públiques catalanes.

Actualment existeixen set entitats de certificació vinculades a la jerarquia pública de certificació de les administracions públiques catalanes: EC-GENCAT, EC-SAFP, EC-AL, EC-idCAT, EC-UR, EC-URV i EC-Parlament.

### 1.1.1 Tipus i classes de certificats

L'EC-ACC ha definit una tipologia de serveis de certificació, que li permeten emetre certificats digitals per a diversos usos i usuaris finals diferents.

Els certificats d'infraestructura són aquells que s'emeten per gestionar i operar la infraestructura de clau pública (PKI), que és el sistema tècnic, jurídic, de seguretat i d'organització que ofereix suport als serveis de certificació i de signatura electrònica.

L'EC-ACC emet els següents tipus de Certificats d'infraestructura:

- 1) Certificat d'infraestructura d'entitat de certificació vinculada (CIC), que s'expedeix a les Entitats de Certificació que es vinculen a la jerarquia.

Les Entitats de Certificació vinculades poden, al seu torn, emetre certificats d'infraestructura o certificats d'entitat final (personals, d'entitat i de dispositiu), segons la classe del certificat CIC que posseeixin, des del moment en el qual hagin obtingut un certificat CIC vàlid, i mentre l'esmentat certificat sigui vigent.

- 2) Certificat d'infraestructura personal de 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.
- 3) Certificat d'infraestructura de dispositiu servidor segur (CIDS), que utilitza 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.
- 4) Certificat d'infraestructura de dispositiu d'aplicació digitalment assegurada (CIDA), que s'utilitza 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.
- 5) Certificat d'infraestructura de servidor d'estat de certificats en línia (CIO), que utilitza un servidor OCSP Responder per signar les seves respostes sobre l'estat de validesa dels certificats.

- 6) Certificat d'infraestructura d'entitat de segells de temps (CIT), que utilitza una entitat per signar els segells de temps que emet.
- 7) Certificat d'infraestructura d'entitat de validació (CIV), que utilitza un servidor d'entitat de validació per signar els seus informes.

#### 1.1.1.1 Certificat d'infraestructura d'entitat de certificació vinculada (CIC), que s'expedeix a les Entitats de Certificació que es vinculen a la jerarquia

Els certificats CIC són aquells certificats d'infraestructura emesos únicament a altres Entitats de Certificació que, d'aquesta forma, queden vinculades a la jerarquia pública de certificació de Catalunya.

Els certificats CIC s'expedeixen per oferir serveis a una comunitat d'usuaris concreta dins de la jerarquia pública de certificació de Catalunya i poden ser de diferents nivells (nivell 1, 2 o successius).

Amb aquests certificats, es faculta a les Entitats de Certificació a emetre certificats a usuaris finals o a altres Entitats de Certificació dins de la seva pròpia comunitat d'usuaris, en funció de les seves necessitats concretes i sempre que tècnicament no afecti el funcionament, plataformes, sistemes i aplicacions emprats habitualment pels usuaris finals.

Cada certificat CIC rep un nivell, adequat al seu període de durada, que s'utilitzarà per a la programació de la renovació periòdica de la infraestructura de certificació.

Aquests certificats permeten que les Entitats de Certificació subscriptores puguin expedir certificats a altres usuaris, ja siguin altres Entitats de Certificació de nivell inferior dins de la jerarquia, com entitats finals (personals, d'entitat, de dispositiu i d'objecte), des del moment en què hagin obtingut un certificat CIC vàlid i mentre aquest certificat sigui vigent.

Aquests certificats generalment són emesos per l'Agència Catalana de Certificació, com a 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.

Aquests certificats CIC s'obtenen després d'un procés d'admissió de l'EC Vinculada als serveis de certificació de l'Agència Catalana de Certificació, procés descrit a la Declaració de Pràctiques de Certificació (DPC) de CATCert.

La futura EC Vinculada no podrà sol·licitar el Certificat CIC fins que no hagi completat el seu procediment d'admissió en la Jerarquia d'Entitats de Certificació de Catalunya d'acord amb la DPC de CATCert.

Atenent al nivell de l'Entitat de Certificació a la qual s'emet el Certificat CIC, es distingeixen els següents tipus de Certificats:

##### a. Certificat d'Infraestructura d'Entitat de Certificació Arrel (CIC Arrel)

El Certificat CIC Arrel és el certificat que l'Agència Catalana de Certificació s'expedeix de forma exclusiva a si mateixa com a Entitat de Certificació Arrel de la Jerarquia pública de certificació de Catalunya per emetre i gestionar els certificats de les Entitats de Certificació Vinculades a l'esmentada Jerarquia.

La durada de la llicència del CIC de l'EC-ACC és de vint-i-vuit (28) anys, a comptar des de la data de la seva emissió.

##### b. Certificat d'Infraestructura de l'Entitat de Certificació de nivell 1

La durada de la llicència dels CIC de nivell 1 és de vint-i-quatre (24) anys, a comptar des de la data de la seva emissió.

Dins d'aquest tipus d'entitats de certificació vinculades es troba l'Entitat de Certificació de la Generalitat de Catalunya (EC-GENCAT), que s'encarrega de la prestació de serveis de certificació a la comunitat d'usuaris de la Generalitat de Catalunya.

### **c. Certificat d'Infraestructura de l'Entitat de Certificació de nivell 2**

La durada de la llicència dels CIC de nivell 2 és de setze (16) anys, a comptar des de la data de la seva emissió.

D'entre les entitats de certificació vinculades de nivell 2 es troben:

- l'Entitat de Certificació de la Secretaria d'Administració i Funció Pública (EC-SAFP), que expedeix certificats al personal i als dispositius dels Organismes, Departaments i Empreses Públiques de la Secretaria d'Administració i Funció Pública.
- l'Entitat de Certificació de Ciutadans (EC-idCAT), que expedeix certificats al públic, és a dir, els ciutadans i ciutadanes catalans, així com a altres persones (anomenats col·lectivament subscriptors) que necessiten relacionar-se amb les Administracions públiques i altres institucions.
- l'Entitat de Certificació de l'Administració Local (EC-AL), els certificats dels quals s'expedeixen al públic, al personal i als dispositius dels Ajuntaments, Consells comarcals, Diputacions, així com a Organismes Autònoms i a Empreses Públiques dels anteriors.
- l'Entitat de Certificació d'Universitats i Recerca (EC-UR), els certificats dels quals es destinen al personal, als estudiants i als dispositius de les universitats i dels centres d'investigació de Catalunya, en el seu cas, connectats a l'"Anella Científica".
- l'Entitat de Certificació del Parlament de Catalunya (EC-Parlament), els certificats dels quals s'expedeixen als Parlamentaris i al Personal d'Administració i Serveis del Parlament de Catalunya, als Síndics i al Personal d'Administració i als Serveis de la Sindicatura de Comptes, als dispositius del Parlament de Catalunya; i al personal assessor dels partits polítics o grups parlamentaris dins de la infraestructura del Parlament de Catalunya.

### **d. Certificat d'Infraestructura de l'Entitat de Certificació de nivell 3**

La durada de la llicència dels CIC de nivell 3 és de vuit (8) anys, a comptar des de la data de la seva emissió.

Actualment, l'única entitat de certificació vinculada de nivell 3 és l'Entitat de Certificació d'Universitat Rovira i Virgili (EC-URV), que expedeix certificats al personal, als estudiants i als dispositius de les facultats i dels centres universitaris de la Universitat Rovira i Virgili.

#### **1.1.1.2 Certificat d'infraestructura personal de signatura electrònica reconeguda d'operadors (CIPISR)**

Els CIPISR són certificats d'infraestructura 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.

En conseqüència, aquests certificats s'utilitzen únicament per autoritzar operacions relacionades amb els serveis de certificació, com l'aprovació de sol·licituds de certificació, i no es poden utilitzar per a cap altre ús que no sigui el d'operador d'Entitat de Registre.

Els CIPISR s'emeten en dues modalitats: de classe 1 i de classe 2. Els CIPISR de classe 1 s'expedeixen a operadors d'Entitats de Registre en l'àmbit de les institucions integrants del sector públic català, mentre que els CIPISR de classe 2 s'expedeixen a operadors d'entorns tancats d'usuaris en l'àmbit privat.

La durada de la llicència dels CIPISR, de classe 1 i 2, és de quatre (4) anys, a comptar des de la data de la seva emissió.

#### 1.1.1.3 Certificat d'infraestructura de dispositiu servidor segur (CIDS)

Els CIDS són certificats d'infraestructura emesos a Entitats de Certificació responsables de l'operació de servidors segurs SSL o TLS amb la finalitat d'identificar-se davant de les aplicacions client que es connecten i la protecció del secret de les comunicacions entre el client i el servidor.

Els certificats CIDS es caracteritzen pel fet que el posseïdor de la clau privada és un dispositiu informàtic que realitza les operacions de signatura i desxifrat de forma automàtica, sota la responsabilitat del subscriptor del certificat.

Els certificats CIDS són certificats destinats a ser utilitzats exclusivament en un servidor del subscriptor identificat en el propi certificat, que l'identifiquen electrònicament i protegeixen la informació entre el client i el servidor. Per això, és condició essencial per a la validesa del certificat CIDS l'especificació dels sistemes del subscriptor en els quals s'utilitzaran els certificats.

La durada de la llicència dels CIDS és de quatre (4) anys, a comptar des de la data de la seva emissió.

#### 1.1.1.4 Certificat d'infraestructura de dispositiu d'aplicació digitalment assegurada (CIDA)

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

Com a certificat de dispositiu, els certificats CIDA es caracteritzen pel fet que el posseïdor de la clau privada és un dispositiu informàtic que realitza les operacions de signatura i desxifrat de forma automàtica, sota la responsabilitat del subscriptor del certificat.

Els certificats CIDA són certificats destinats a ser utilitzats exclusivament en un dispositiu del subscriptor identificat en el propi certificat i, per tant, en els sistemes del subscriptor del certificat.

La durada de la llicència dels CIDA és de quatre (4) anys, a comptar des de la data de la seva emissió.



#### 1.1.1.5 Certificat d'infraestructura de servidor d'estat de certificats en línia (CIO)

Els certificats CIO són aquells certificats d'infraestructura, emesos per gestionar els serveis de certificació, que s'expedeixen a Entitats responsables de l'operació de servidors OCSP Responder, per signar les seves respostes sobre l'estat de validesa dels certificats.

Els certificats CIO són certificats destinats a ser utilitzats exclusivament en un servidor OCSP Responder de l'Entitat subscriptora, servidor que es troba identificat en el propi certificat. Per això, és condició essencial per a la validesa del certificat CIO l'especificació dels sistemes del subscriptor en els quals s'utilitzaran els certificats.

La durada de la llicència dels CIO és de quatre (4) anys, a comptar des de la data de la seva emissió.

#### 1.1.1.6 Certificat d'infraestructura d'entitat de segells de temps (CIT), que és utilitzat per una entitat per signar els segells de temps que emet

Els certificats CIT són certificats expedits a les Entitats responsables de l'operació d'autoritats de segellat de temps i hora (d'ara endavant, TSA) que s'utilitzen per signar els segells de temps que emeten aquestes autoritats.

Els CIT són certificats ordinaris que serveixen per gestionar els serveis de certificació i per garantir la data i l'hora d'un acte determinat.

La durada de la llicència dels CIT és de quatre (4) anys, a comptar des de la data de la seva emissió.

Els certificats CIT són emesos exclusivament perquè les Entitats subscriptors signin els segells de temps que emeten.

#### 1.1.1.7 Certificat d'infraestructura d'entitat de validació (CIV)

Els certificats CIV són certificats d'infraestructura, emesos per gestionar els serveis de certificació, que s'expedeixen a Entitats de Validació perquè signin els informes de validació que emeten.

El certificat CIV ofereix, respecte dels Informes de Validació signats amb aquest certificat, les garanties següents:

- Garantia de verificació dels certificats o signatures respecte dels quals s'hagi realitzat la sol·licitud de l'Informe de Validació.
- Garantia del contingut dels esmentats certificats o signatures prèviament verificats.
- Garantia de la data i hora de l'informe.

La durada de la llicència dels CIV és de quatre (4) anys, a comptar des de la data de la seva emissió.

Adicionalment, en funció dels requeriments tècnics i de les necessitats dels usuaris, és possible que els esmentats tipus de certificats puguin incorporar altres funcionalitats que, en tot cas, s'identificaran a 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'Agència Catalana de Certificació (EC-ACC).

L'EC-ACC emet certificats dins de la Jerarquia pública de certificació 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.

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

Aquesta DPC es relaciona amb documentació auxiliar, entre la qual es troben els instruments jurídics reguladors de la prestació del servei, de la documentació i de les polítiques de seguretat, així com de la documentació d'operacions.

## 1.2 Nom del document i identificació

### 1.2.1 Identificació d'aquest document

Aquest document es denomina "Declaració de Pràctiques de Certificació (DPC) d'Infraestructura de CATCert".

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

1.3.6.1.4.1.15096.1.2.2.

### 1.2.2 Identificació de polítiques de certificació cobertes per aquesta DPC

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

- **CIC.-** Certificat d'infraestructura d'entitat de certificació vinculada:
  - Els CIC de nivell 0 s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.10.
    - **Certificat d'Infraestructura d'Entitat de Certificació Arrel (CIC Arrel)**  
El certificat CIC Arrel s'identifica amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.10.
  - Els CIC de nivell 1 s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.11.
    - **Certificat d'Infraestructura de l'Entitat de Certificació de la Generalitat de Catalunya (EC-GENCAT)**  
El certificat CIC de l'EC-GENCAT és de nivell 1 i s'identifica amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.11.

- Els CIC de nivell 2 s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- **Certificat d'Infraestructura de l'Entitat de Certificació de la Secretaria d'Administració i Funció Pública (EC-SAFP)**

El certificat CIC de l'EC-SAFP és de nivell 2 i s'identifica amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- **Certificat d'Infraestructura de l'Entitat de Certificació de Ciutadans (EC-idCAT)**

El certificat CIC de l'EC-idCAT és de nivell 2 i s'identifica amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- **Certificat d'Infraestructura de l'Entitat de Certificació de l'Administració Local (EC-AL)**

El certificat CIC de l'EC-AL és de nivell 2 i s'identifica amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- **Certificat d'Infraestructura de l'Entitat de Certificació d'Universitats i Recerca (EC-UR)**

El certificat CIC de l'EC-UR és de nivell 2 i s'identifica amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- a) Certificat d'Infraestructura de l'Entitat de Certificació del Parlament de Catalunya (EC-Parlament)**

El certificat CIC de l'EC-Parlament és de nivell 2 i s'identifica amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- Els CIC de nivell 3 s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.13.

- **Certificat d'Infraestructura de l'Entitat de Certificació d'Universitat Rovira i Virgili (EC-URV)**

El certificat CIC de l'EC-URV és de nivell 3 i s'identifica amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.13.

- **CIPISR.- Certificat d'infraestructura personal de signatura electrònica reconeguda d'operadors.**

Els certificats CIPISR de classe 1 emesos per CATCert s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.15.

Els certificats CIPISR de classe 2 emesos per CATCert s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.16.

- **Certificat d'infraestructura de dispositiu servidor segur (CIDS).**

Els certificats CIDS de classe 1 emesos per CATCert s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.17.

- **Certificat d'infraestructura de dispositiu d'aplicació digitalment assegurada (CIDA).**

Els certificats CIDA de classe 1 emesos per CATCert s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.18.

- **Certificat d'infraestructura de servidor d'estat de certificats en línia (CIO).**

Els certificats CIO de classe 1 emesos per CATCert s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.19.

- **Certificat d'infraestructura d'entitat de segells de temps (CIT), que és utilitzat per una entitat per signar els segells de temps que emet.**

Els certificats CIT de classe 1 emesos per CATCert s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.111.

- **Certificat d'infraestructura d'entitat de validació (CIV).**

Els certificats CIV de classe 1 emesos per CATCert s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.20.

## 1.3 Comunitat d'usuaris de certificats

Aquesta 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 d'infraestructura de l'EC-ACC no s'expedeixen al públic, sinó a:

- La pròpia Entitat de Certificació Arrel de la jerarquia (EC-ACC).
- L'Entitat de Certificació de la Generalitat de Catalunya (EC-GENCAT).
- L'Entitat de Certificació de la Secretaria d'Administració Pública.
- L'Entitat de Certificació de Ciutadans (EC-Citadas).
- L'Entitat de Certificació de l'Administració Local (EC-AL).
- L'Entitat de Certificació de la Universitat i Recerca (EC-UR).
- L'Entitat de Certificació de la Universitat Rovira i Virgili (EC-URV).
- L'Entitat de Certificació del Parlament de Catalunya (EC-Parlament).

### 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.

CATCert és el prestador de serveis de certificació arrel de la jerarquia d'entitats de certificació de les entitats públiques de Catalunya.

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

### 1.3.2 Entitat de Certificació Arrel

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

L'esmentada vinculació tècnica s'aconsegueix mitjançant l'emissió de certificats d'infraestructura d'entitat de certificació vinculada (CIC).

### 1.3.3 Entitats de Certificació Vinculades

Les Entitats de Certificació Vinculades són les institucions, a les quals el prestador del servei de certificació presta els serveis d'expedició i de gestió dels certificats mitjançant les autoritats de certificació, i que es troben inscrites a la jerarquia pública de certificació de Catalunya.

Amb una Entitat de Certificació Vinculada, la institució emet certificats a altres entitats de certificació vinculades o a usuaris finals, mitjançant l'emissió dels certificats d'infraestructura, personals, d'entitat, de dispositius i d'objectes.

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

CATCert pot crear, al seu torn, Entitats de Certificació Vinculades de la seva pròpia titularitat quan no existeixi una institució única responsable d'una comunitat d'usuaris que precisen certificats.

### 1.3.4 Entitats de Registre

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

### 1.3.5 Usuaris finals

Els usuaris finals són les persones que obtenen i utilitzen els certificats emesos per l'EC-ACC. En concret, es poden distingir els usuaris finals següents:

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

#### 1.3.5.1 Sol·licitants de certificats

Els sol·licitants dels certificats indicats en aquesta DPC són les persones autoritzades per les Entitats de Certificació subscriptora.

Poden ser sol·licitants:

- La persona que serà el futur posseïdor de claus.
- Una persona autoritzada per:
  - o L'Entitat de Certificació Arrel de la jerarquia (EC-ACC).
  - o L'Entitat de Certificació de la Generalitat de Catalunya (EC-GENCAT).
  - o L'Entitat de Certificació de la Secretaria d'Administració Pública (EC-SAFP).
  - o L'Entitat de Certificació de Ciutadans (EC-IdCAT).
  - o L'Entitat de Certificació de l'Administració Local (EC-AL).
  - o L'Entitat de Certificació de la Universitat i Recerca (EC-UR).
  - o L'Entitat de Certificació de la Universitat Rovira i Virgili (EC-URV).
  - o L'Entitat de Certificació del Parlament de Catalunya (EC-Parlament).

L'autorització es podrà realitzar de forma expressa o tàcita i, en aquells casos en els quals l'EC-ACC ho consideri convenient, s'haurà de formalitzar documentalment.

#### 1.3.5.2 Subscriptors de certificats

Els subscriptors dels certificats són les institucions i les persones, físiques o jurídiques, que s'identifiquen en el camp "Subject" del certificat.

El subscriptor dels certificats d'infraestructura és:

- L'Entitat de Certificació Arrel de la jerarquia (EC-ACC).
- L'Entitat de Certificació de la Generalitat de Catalunya (EC-GENCAT).
- L'Entitat de Certificació de la Secretaria d'Administració Pública.
- L'Entitat de Certificació de Ciutadans (EC-Citadas).
- L'Entitat de Certificació de l'Administració Local (EC-AL).
- L'Entitat de Certificació de la Universitat i Recerca (EC-UR).
- L'Entitat de Certificació de la Universitat Rovira i Virgili (EC-URV).
- L'Entitat de Certificació del Parlament de Catalunya (EC-Parlament).

#### 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, que estan degudament autoritzades per això pel subscriptor i degudament identificades al certificat mitjançant el seu nom i cognoms o mitjançant un pseudònim (aquesta última possibilitat s'aplica únicament als certificats de classe 2).

#### 1.3.5.4 Verificadors de certificats

Els verificadors són les persones (s'inclouen les persones físiques, institucions, persones jurídiques i altres organitzacions i entitats) que reben signatures digitals i certificats digitals i han de verificar-los com a pas previ per confiar-hi.

## 1.4 Ús dels certificats

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

### 1.4.1 Usos típics dels certificats

#### 1.4.1.1 Certificat d'infraestructura d'entitat de certificació vinculada (CIC) que s'expedeix a les Entitats de Certificació que es vinculen a la jerarquia

Aquests certificats permeten que les Entitats de Certificació subscriptores puguin expedir certificats a altres usuaris, ja siguin altres Entitats de Certificació de nivell inferior dins de la jerarquia, com entitats finals (personals, d'entitat, de dispositiu i d'objecte), des del moment en què hagin obtingut un certificat CIC vàlid i mentre aquest sigui vigent.

Aquests certificats generalment són emesos per l'Agència Catalana de Certificació, com EC Arrel, a organitzacions que operen una EC dins de la seva jerarquia, per a diferents usos, segons la seva classe:

- Signatura de peticions de renovació, suspensió i revocació de certificats CIC.
- Emissió i signatura de certificats CIC, CIPISR, CIDS, CIDA, CIO, CIT, CIV, CPSR, CPSA, CPISR, CPISA, CPIXSA, CPI, CPX, CESR, CEX, CDS, CDSCD, CDA, CDP i COS.
- Emissió i signatura de llistes de revocació de certificats (LRC).

#### a. Certificat d'Infraestructura d'Entitat de Certificació Arrel (CIC Arrel)

Els usos permesos del certificat CIC de l'EC-ACC són:

- Signatura de peticions de renovació, suspensió i revocació de certificats CIC.
- Emissió i signatura de certificats CIC, CIPISR, CIDS, CIDA, CIO, CIT i CIV.
- Emissió i signatura de llistes de revocació de certificats (LRC).

#### b. Certificat d'Infraestructura de l'Entitat de Certificació de la Generalitat de Catalunya (EC-GENCAT)

Els usos permesos del certificat CIC de l'EC-GENCAT són:

- Emissió i signatura de certificats CIC, CIPISR, CIDS, CIDA, CIT, CIO i CIV.
- Emissió i signatura de llistes de revocació de certificats (LRC).

#### c. Certificat d'Infraestructura de l'Entitat de Certificació de la Secretaria d'Administració i Funció Pública (EC-SAFP)

Els usos permesos del certificat CIC de l'EC-SAFP són:

- Emissió i signatura de certificats: CPISR-1, CPX-1, CPISR-1 Càrrec Ús, CPISR-1 Càrrec, CPX-1 Càrrec, CPISR-2 Càrrec, CPX-2 Càrrec, CEISR-1, CEX-1, CIPISR-1, CIPISR-2, CDS-1, CDSCD-1, CDS-1 Seu electrònica, CDP-1 i CDA-1 i CDA-1 Segell electrònic, CIPISR-1 y CIPISR-2.
- Emissió i signatura de llistes de revocació de certificats (LRC).



**d. Certificat d'Infraestructura de l'Entitat de Certificació de Ciutadans (EC-idCAT)**

Els usos permesos del certificat CIC de l'EC-idCAT són:

- Emissió i signatura de certificats CPISA i CPIXSA.
- Emissió i signatura de llistes de revocació de certificats (LRC).

**e. Certificat d'Infraestructura de l'Entitat de Certificació de l'Administració Local (EC-AL)**

Els usos permesos del certificat CIC de l'EC-AL són:

- Emissió i signatura de certificats CPISR-1, CPX-1, CPISR-1 Càrrec Ús, CPISR-1 Càrrec, CPX-1 Càrrec, CPISR-2 Càrrec, CPX-2 Càrrec, CEISR-1, CEX-1, CIPIISR-1, CIPIISR-2, CDS-1, CDSCD-1, CDS-1 Seu electrònica, CDP-1 i CDA-1 i CDA-1 Segell electrònic, CIPIISR-1 y CIPIISR-2.
- Emissió i signatura de llistes de revocació de certificats (LRC).

**f. Certificat d'Infraestructura de l'Entitat de Certificació d'Universitats i Recerca (EC-UR)**

Els usos permesos del certificat CIC de l'EC-UR són:

- Emissió i signatura de certificats CPISR-1 Càrrec, CPISR-1 Càrrec Estranger, CPX-1 Càrrec, CPX-1 Càrrec Estranger, CPX-1 Càrrec, CPISR-2 Càrrec, CPX-2 Càrrec, CPISR-2 Estudiant, CPX-2 Estudiant, CPISR-2 Estudiant Estranger, CPISR-2 Estudiant Estranger, CEISR-1, CEX-1, CDS-1, CDSCD-1, CDS-1 Seu electrònica, CDP-1, CDA-1, CDA-1 Segell electrònic, CIPIISR-1 i CIPIISR-2.
- Emissió i signatura de llistes de revocació de certificats (LRC).

**g. Certificat d'Infraestructura de l'Entitat de Certificació d'Universitat Rovira i Virgili (EC-URV)**

Els usos permesos del certificat CIC de l'EC-URV són:

- Emissió i signatura de certificats CPISR-1 Càrrec, CPISR-1 Càrrec Estranger, CPX-1 Càrrec, CPX-1 Càrrec Estranger, CPISR-2 Càrrec, CPX-2 Càrrec, CPISR-2 Estudiant, CPX-2 Estudiant, CPISR-2 Estudiant Estranger, CPISR-2 Estudiant Estranger, CEISR-1, CEX-1, CDS-1, CDSCD-1, CDS-1 Seu electrònica, CDP-1, CDA-1, CDA-1 Segell electrònic, CIPIISR-1 i CIPIISR-2.
- Emissió i signatura de llistes de revocació de certificats (LRC).

**h. Certificat d'Infraestructura de l'Entitat de Certificació del Parlament de Catalunya (EC-Parlament)**

Els usos permesos del certificat CIC de l'EC-Parlament són:

- Emissió i signatura de certificats CPISR-1 Càrrec, CPX-1 Càrrec, CPISR-2 Càrrec, CPX-2 Càrrec, CEISR-1, CEX-1, CDS-1, CDSCD-1, CDS-1 Seu electrònica, CDA-1, CDA-1 Segell electrònic, CDP-1, CIPIISR-1 i CIPIISR-2.
- Emissió i signatura de llistes de revocació de certificats (LRC).

#### 1.4.1.2 Certificat d'infraestructura personal de signatura electrònica reconeguda d'operadors (CIPISR)

Aquests Certificats permeten que els operadors d'Entitats de Registre realitzin els treballs d'emissió i de gestió del cicle de vida de certificats d'una Entitat de Certificació.

Per consegüent, aquests certificats s'utilitzen únicament per autoritzar operacions relacionades amb els serveis de certificació, com l'aprovació de sol·licituds de certificació, i no es poden utilitzar per a cap altre ús que no sigui el d'operador d'Entitat de Registre.

#### 1.4.1.3 Certificat d'infraestructura de dispositiu servidor segur (CIDS)

Aquests Certificats permeten que les Entitats de Certificació responsables de l'operació de servidors segurs SSL o TLS:

- S'identifiquin davant de les aplicacions client que es connectin,
- Protegeixin el secret de les comunicacions entre el client i el servidor.

Els Certificats CIDS estan destinats a ser utilitzats exclusivament en un servidor del subscriptor identificat en el propi certificat, que l'identifiquen electrònicament i protegeixen la informació entre el client i el servidor. Per això, és condició essencial per a la validesa del certificat CIDS l'especificació dels sistemes del subscriptor en els quals s'utilitzaran els certificats.

#### 1.4.1.4 Certificat d'infraestructura de dispositiu d'aplicació digitalment assegurada (CIDA)

Aquests Certificats permeten que les Entitats de Certificació responsables de l'operació d'aplicacions informàtiques que s'identifiquen digitalment signin electrònicament *webservices* o altres protocols i rebin documents i missatges xifrats.

Els Certificats CIDA estan destinats a ser utilitzats exclusivament en un dispositiu del subscriptor identificat en el propi certificat i, per tant, en els sistemes del subscriptor del certificat.

#### 1.4.1.5 Certificat d'infraestructura de servidor d'estat de certificats en línia (CIO)

Aquests Certificats permeten que les Entitats responsables de l'operació de servidors OCSP Responder signin les seves respostes sobre l'estat de validesa dels certificats.

Els certificats CIO són certificats destinats a ser utilitzats exclusivament en un servidor OCSP Responder de l'Entitat subscriptora, servidor que es troba identificat en el propi certificat. Per això, és condició essencial per a la validesa del certificat CIO l'especificació dels sistemes del subscriptor en els quals s'utilitzaran els certificats.

#### 1.4.1.6 Certificat d'infraestructura d'entitat de segells de temps (CIT)

Aquests Certificats permeten que les Entitats responsables de l'operació d'autoritats de segellat de temps i hora (d'ara endavant, TSA) signin els segells de temps que aquestes Entitats emeten.

Els CIT són certificats ordinaris que serveixen per gestionar els serveis de certificació i per garantir la data i l'hora d'un acte determinat.



#### 1.4.1.7 Certificat d'infraestructura d'entitat de validació (CIV)

Aquests Certificats permeten que les Entitats de Certificació, actuant com a Entitats de Validació, signin els informes de validació que emeten.

### 1.4.2 Aplicacions prohibides

#### 1.4.2.1 Aplicacions prohibides per a tots els tipus de certificats

Els certificats només es podran utilitzar dins dels límits d'ús recollits d'una manera expressa en la seva llicència d'ús i les seves corresponents Condicions d'Ús. Qualsevol altre ús fora dels descrits en els esmentats documents, queden exclosos expressament de l'àmbit contractual i prohibits formalment.

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

#### 1.4.2.2 Requisits específics per als CIC

Els certificats CIC s'atendran a allò que es disposa en aquesta DPC i, en tot cas, les limitacions estaran delimitades per la classe de certificat CIC i per la política del certificat en qüestió.

#### 1.4.2.3 Requisits específics per als CIPISR

Els CIPISR no es poden utilitzar per a cap altre ús que no sigui el d'operador d'Entitat de Registre.

#### 1.4.2.4 Requisits específics per als CIDS, CIDA, CIO, CIT i CIV

Els CIDS, CIDA, CIO, CIT i CIV no es poden utilitzar en sistemes diferents dels d'Entitat de Certificació.

## 1.5 Administració de la Declaració de Pràctiques

### 1.5.1 Organització que administra l'especificació

CATCert - Agència Catalana de Certificació

Passatge de la Concepció, 11

08008 - Barcelona

Telèfon: 93 272 26 00

Fax: 93 272 25 39

Correu electrònic: [info@catcert.net](mailto:info@catcert.net)

Telèfon d'assistència:

902 901 080

### 1.5.2 Dades de contacte de l'organització

CATCert - Agència Catalana de Certificació

Passatge de la Concepció, 11

08008 - Barcelona

Telèfon: 93 272 26 00

Fax: 93 272 25 39

Correu electrònic: info@catcert.net

Telèfon d'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.net

Telèfon d'assistència:

902 901 080

### 1.5.4 Procediment d'aprovació

El sistema documental i d'organització de l'EC-ACC garanteix, mitjançant l'existència i l'aplicació dels corresponents procediments, el manteniment correcte d'aquesta DPC i de les especificacions de servei que hi estan relacionades.

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

## 2. Publicació d'informació i directori de certificats

### 2.1 Directori de certificats

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

### 2.2 Publicació d'informació de l'EC-ACC

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

- Les llistes de certificats revocats i altres informacions d'estat de revocació dels certificats.
- La política general de certificació i, quan sigui convenient, les polítiques específiques.
- Els perfils dels certificats i de les llistes de revocació dels certificats.
- La Declaració de Pràctiques de Certificació.
- Els instruments jurídics vinculants amb subscriptors i verificadors.

Qualsevol canvi en les especificacions o en les condicions del servei es comunica als usuaris per l'EC-ACC a través del directori.

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

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

### 2.3 Freqüència de publicació

La informació de l'EC-ACC 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 d'aquesta DPC es regeixen per l'establert a la secció 9.12.1.

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

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

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

## 2.4 Control d'accés

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

L'EC-ACC 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.
- Els certificats només siguin accessibles en els supòsits o a les persones que el signant indiqui.
- Detecti qualsevol canvi tècnic que afecti els requisits de seguretat.

## 3. Identificació i autenticació

### 3.1 Gestió de noms

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

#### 3.1.1 Tipus de noms

##### 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 els seu significat semàntic, es troben descrits en el document "perfil de certificat" corresponent que CATCert publica al seu web (<http://www.catcert.cat/>).

##### 3.1.1.2 Perfils dels certificats

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

#### 3.1.2 Significat dels noms

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

La identificació de les persones físiques (posseïdors de claus) està formada pel seu nom i cognoms juntament amb el seu NIF.

#### 3.1.3 Utilització d'anònims i pseudònims

No es poden utilitzar pseudònims per identificar una organització.

#### 3.1.4 Interpretació de formats de noms

Sense estipulació addicional.

#### 3.1.5 Unicitat dels noms

L'EC-ACC emet diferents tipus de certificats. Els noms dels subscriptors de certificats són únics per a cada servei de generació de certificats operat per l'EC-ACC 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-ACC.

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

### 3.1.6 Resolució de conflictes relatius a noms

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

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

Així mateix, l'EC-ACC no actua com a àrbitre o mitjancer, ni de cap altra manera resol cap disputa concernent 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-ACC es reserva el dret de refusar una sol·licitud de certificat per causa de conflicte de nom.

En referència al tractament de marques registrades, s'està d'acord amb allò que es disposa a l'apartat 9.5.3 d'aquesta DPC.

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

- En cas de nacionals espanyols, el DNI del posseïdor de claus.  
V.gr.: (C) = ES; (SN) = DNI
  - En cas d'estrangers amb algun tipus de vinculació amb Espanya com pot ser la residència a territori espanyol, el NIE del posseïdor de claus.  
V.gr.: francès (C) = ES; (SN) = NIE  
V.gr.: argentí (C) = ES; (SN) = NIE
  - En cas d'estrangers nacionals d'Estats que formen part de l'Acord Schengen i que manquen 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 formen part de l'Acord Schengen i que manquen de NIE, el Passaport ordinari, diplomàtic, oficial o de servei, del posseïdor de claus vàlidament expedit i en vigor.  
V.gr.: xinès (C) = ES; (SN) = CN-Passaport.
- En els dos supòsits anteriors, juntament amb els identificadors esmentats, es col·locarà el codi del país del qual 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 les Entitats de Certificació, identificades 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, d'entre altres, l'atribut "countryName", el valor del qual consisteix a especificar el context en el qual s'han d'entendre definits els demés 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, al voltant de la seva nacionalitat. Per tant, per determinar el “SerialNumber” del “Subject” s’aplica la normativa reguladora de la nacionalitat i de l’estrangeria d’un determinat Estat, en aquest cas, de l’Estat Espanyol.

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

Aquells estrangers que manquen de NIE s’identifiquen amb la corresponent documentació acreditativa, que varia en funció de la seva nacionalitat, i s’estableix una diferència entre els nacionals d’Estats que formen part de l’Acord Schengen i la resta. Els primers acrediten la seva identitat mitjançant la presentació del seu document nacional d’identitat o del seu passaport vàlidament expedit i en vigor. I, els segons, l’acrediten mitjançant el passaport, el títol de viatge, el document nacional d’identitat, cèdula d’identificació o qualsevol altre document que acrediti la seva identitat en virtut de compromisos internacionals, en els quals quedin perfectament reflectides la identitat i la nacionalitat del titular del document.

## 3.2 Validació inicial de la identitat

### 3.2.1 Prova de possessió de clau privada

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

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

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

### 3.2.2 Autenticació de la identitat d’una Organització

#### 3.2.2.1 Entitats de Certificació Vinculades

No es requereix realitzar procediment d’autenticació de les Entitats de Certificació Vinculades a la jerarquia pública de certificació de CATCert, ja que aquestes es creen en el si de la jerarquia mitjançant un procediment aprovat per la pròpia EC-ACC denominat “Cerimònia de Claus”, descrit a la secció corresponent d’aquesta DPC.

#### 3.2.2.2 Entitats de Registre

L’EC-ACC autentica, prèviament a l’emissió i al lliurament d’un certificat CIPISR, per a qualsevol dels components d’una Entitat de Registre, la identitat de l’Entitat de Registre i de l’operador conforme a la secció corresponent d’aquesta DPC.

### 3.2.2.3 Subscriptors de Certificats

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

## 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 nombre i tipus de documents necessaris per acreditar la identitat del posseïdor de claus són els que admet l'EC-ACC tal com es recull en la seva normativa específica reguladora.

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

- Nom i cognoms de la persona.
- Nom d'identitat legalment reconegut (DNI, NIE o Passaport).
- Data i lloc de naixement.
- Qualsevol altra informació que es pugui utilitzar per identificar una persona (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 classe 1 i 2 es valida comparant la informació de la sol·licitud amb els registres interns de l'EC-ACC 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.

Es considera que la informació del posseïdor registrada per l'EC-ACC els últims cinc anys està actualitzada.

### 3.2.3.3 Necessitat de presència personal

És necessari validar la identitat del posseïdor de claus amb la seva presència física, que és responsabilitat de la pròpia EC-ACC, i que ho fa mitjançant la seva relació funcional, laboral o professional, segons procedeixi.

### 3.2.3.4 Vinculació de la persona física amb l'organització subscriptora

#### • Requisits per a certificats de classe 1

Com que es tracta de certificats corporatius, en els quals l'Entitat de Registre i el subscriptor coincideixen, no és necessari obtenir una justificació documental específica de la vinculació del posseïdor de la clau amb l'Entitat de Registre, sinó que s'utilitzen els registres interns de la Institució.



- Requisits per a certificats de classe 2

L'EC-ACC ha d'obtenir una justificació documental de la vinculació de la persona física amb l'organització, mitjançant qualsevol mitjà admès en dret.

L'EC-ACC pot utilitzar Entitats de Registre per a aquesta tasca.

### 3.2.4 Informació no verificada

L'EC-ACC es responsabilitza que tota la informació inclosa a la sol·licitud del certificat sigui exacta, completa per a la finalitat del certificat. No obstant això, els certificats poden incloure informació no verificada, com per exemple l'adreça de correu electrònic, sempre que s'indiqui als usuaris finals en el propi 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

Se seguirà el mateix procés que per a l'emissió de certificats. Si més no, si la renovació es realitza durant els 5 primers anys des de la primera comprovació de la identitat, aquesta identificació no serà necessària.

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

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

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

## 3.4 Identificació i autenticació de la sol·licitud de revocació

L'EC-ACC haurà d'autenticar les peticions i els informes relatius a la revocació d'un certificat, comprovant que provenen d'una font autoritzada.

## 3.5 Autenticació d'una petició de suspensió

La petició de suspensió es realitzarà per part del subscriptor o, en el seu cas, el posseïdor de claus accedint al web de CATCert i utilitzant el formulari de suspensió que es troba vigent en el moment de realitzar la petició, o bé per telèfon, on se li formularan les preguntes necessàries per identificar la seva identitat.

## 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 sol·licitar l'emissió

##### 4.1.1.1 Requisits generals

Únicament poden sol·licitar certificats d'infraestructura les Entitats de Certificació Vinculades a la jerarquia pública de certificació de Catalunya, operada per CATCert.

##### 4.1.1.2 Requisits específics per al Certificat CIC

La futura Entitat de Certificació no podrà sol·licitar el Certificat CIC fins que no hagi completat el seu procediment d'admissió, a la Jerarquia d'Entitats de Certificació de l'Agència Catalana de Certificació.

#### 4.1.2 Procediment d'alta; Responsabilitats

L'EC-ACC, amb caràcter previ a l'emissió d'un certificat, s'assegura que les sol·licituds de certificats estiguin completes, precises i degudament autoritzades.

Abans de l'emissió i lliurament d'un certificat, l'EC-ACC informará el subscriptor o, en el seu cas, el posseïdor de claus dels termes i condicions aplicables al certificat. Aquest requisit es compleix mitjançant el lliurament de l'instrument jurídic que vincula l'EC-ACC amb el subscriptor o el full de lliurament al posseïdor de claus, en el qual s'inclourà l'esmentada informació. Aquesta informació es comunicarà en suport perdurable, en paper o electrònicament, i en llenguatge fàcilment comprensible.

### 4.2 Processament de la sol·licitud de certificació

#### 4.2.1 Requisits per a tot tipus de certificats

Un cop ha tingut lloc una petició de certificat, l'EC-ACC, a través d'una persona autoritzada, verifica la informació proporcionada conforme als requisits previstos en aquesta DPC.

- Si la verificació no és correcta, l'EC-ACC denega la petició. En el supòsit que les irregularitats no es puguin corregir, l'EC-ACC denega la sol·licitud definitivament.
- Si la verificació és correcta, l'EC-ACC:
  - Aprova la sol·licitud.

- Genera, en el seu cas, el parell de claus i el certificat.

## 4.2.2 Requisits addicionals per al Certificat CIC

Quan l'Entitat de Certificació que sol·licita ser vinculada a la jerarquia pública de certificació de Catalunya no estigui operada per CATCert, es comprovarà, abans d'emetre el certificat, que el prestador de serveis de certificació corresponent pugui demostrar la fiabilitat necessària dels seus serveis.

L'EC-ACC comprovarà, en el procés d'admissió de l'Entitat de Certificació, els aspectes següents:

- Que les polítiques i procediments operats per l'Entitat de Certificació no són discriminatoris.
- Que l'Entitat de Certificació oferirà els seus serveis a tots els seus sol·licitants, les activitats de les quals entren en l'àmbit d'operació declarat a la seva DPC, d'acord amb l'establert a la secció 1.3 de la Política General de Certificació de CATCert.
- Que l'Entitat de Certificació és una entitat legal, d'acord amb l'establert a la secció 1.3.1 de la Política General de Certificació de CATCert, dada que s'autenticarà d'acord amb l'establert a la secció corresponent la Política General de Certificació de CATCert.
- Que l'Entitat de Certificació disposa de sistemes de gestió de la qualitat i la seguretat adequats per a la prestació del servei, dada que es comprovarà en l'auditoria de conformitat prevista a la secció 8 de la Política General de Certificació de CATCert.
- Que l'Entitat de Certificació utilitza personal qualificat i amb l'experiència necessària per a la prestació dels serveis oferts, en l'àmbit de la signatura electrònica i els procediments adequats de seguretat i de gestió.
- Que l'Entitat de Certificació compleix els requisits de capacitat financera establerts a la secció 9.2 de la Política General de Certificació de CATCert.
- Que l'Entitat de Certificació compleix els requisits relatius als procediments de resolució de disputes, establerts a la secció 9.13 de la Política General de Certificació de CATCert.
- Que l'Entitat de Certificació ha documentat de manera adequada les relacions jurídiques en virtut de les que externalitza part o la totalitat dels seus serveis.

## 4.3 Emissió de certificat

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

Per a cada sol·licitud de certificat tramitada, l'EC-ACC:

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

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

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 certificat nou.

### 4.3.2 Notificació de l'emissió al subscriptor

L'EC-ACC notifica a CATCert l'emissió del certificat, o la incidència corresponent. Així mateix, s'indicarà la disponibilitat del certificat i la forma d'obtenir-lo.

## 4.4 Acceptació del certificat

### 4.4.1 Responsabilitats del Prestador de Serveis de Certificació

L'EC-ACC:

- Si no ho ha fet abans, i quan resulti necessari, acreditarà la identitat del subscriptor.
- Proporcionarà al subscriptor accés al certificat.
- Lliurarà, en el seu cas, el dispositiu criptogràfic de signatura, verificació de signatura, xifrat o desxifrat.
- Proporcionarà la informació següent:
  - Informació bàsica sobre la política i l'ús del certificat, incloent especialment informació sobre l'Entitat de Certificació Vinculada i la Declaració de Pràctiques de Certificació aplicable, així com les seves obligacions, facultats i responsabilitats.
  - Informació sobre el certificat i el dispositiu criptogràfic.
  - Reconeixement del posseïdor de rebre el certificat i, en el seu cas, el dispositiu criptogràfic, i acceptació dels esmentats elements.
  - Obligacions del posseïdor de claus.
  - Responsabilitat de posseïdor de claus.
  - Mètode d'imputació exclusiva al posseïdor de la seva clau privada i de les seves dades d'activació del certificat i, en el seu cas, del dispositiu criptogràfic, d'acord amb l'establert a les seccions corresponents d'aquesta política.
  - La data de l'acte de lliurament i acceptació.

#### 4.4.2 Conducta que constitueix acceptació del certificat

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

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

#### 4.4.3 Publicació del certificat

Els certificats es poden publicar sense el consentiment previ dels posseïdors de claus.

#### 4.4.4 Notificació de l'emissió a tercers

No aplicable.

### 4.5 Ús del parell de claus i del certificat

#### 4.5.1 Ús pels posseïdors de claus

##### 4.5.1.1 Requisits per a tots els tipus de certificats

Els certificats s'utilitzen per permetre una millor seguretat en les comunicacions telemàtiques internes de les Institucions, entre elles, així com les que es realitzin amb la resta de la societat. Els certificats s'utilitzen d'acord amb la seva funció pròpia i finalitat establerta, i no es poden utilitzar en altres funcions o amb altres finalitats.

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

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

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

Tanmateix, es té en compte que es dona la circumstància que l'efectivitat de les limitacions basades en extensions de certificats depèn en ocasions de l'operació d'aplicacions informàtiques que no han estat fabricades ni poden estar controlades per les Entitats de Certificació.

##### 4.5.1.2 Requisits addicionals per als certificats CIC

Els certificats CIC només poden ser utilitzats per a funcions d'Entitat de Certificació, en conjunció amb un dispositiu segur de generació de signatura, d'acord amb els requisits establerts a la Política General de Certificació de CATCert.

## 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 es puguin utilitzar en altres funcions i amb altres finalitats. De la mateixa forma, els certificats s'utilitzen únicament d'acord amb la llei aplicable, especialment tenint en compte les restriccions d'importació i d'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 establir límits tècnics als usos que es pot donar a una clau privada corresponent a una clau pública llistada en un certificat X.509v3.

Així mateix, 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-ACC.

El tercer que confia en els Certificats s'obliga a no utilitzar cap classe d'informació d'estat dels certificats o de cap altre tipus que hagi estat subministrada per CATCert, en la realització.

## 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

Quan es sol·liciti la renovació d'un certificat d'infraestructura, i atès que l'esmentada renovació exigeix al seu torn la renovació de claus, l'EC-ACC verifica que les dades de registre continuen sent vàlides i, si alguna dada ha canviat, aquesta és verificada i guardada.

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

## 4.8 Modificació de certificats

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-ACC pot revocar un certificat per les causes següents:

1. Circumstàncies que afecten la informació continguda al certificat:
  - Modificació d'alguna de les dades contingudes al certificat.
  - Descobriment que alguna de les dades contingudes a la sol·licitud de certificat és incorrecte.
  - Descobriment que alguna de les dades contingudes al certificat és incorrecte.
2. Circumstàncies que afecten a la seguretat de la clau o del certificat:
  - Compromís de la clau privada o de la infraestructura o sistemes de l'EC-ACC, sempre que afecti la confiança en els certificats emesos a partir d'aquest incident.
  - Infracció, per l'EC-ACC, 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.
  - L'ús irregular del certificat pel subscriptor o manca de diligència en la custòdia de la clau privada.
3. Circumstàncies que afecten el dispositiu criptogràfic:
  - Compromís o sospita de compromís de la seguretat del dispositiu criptogràfic.
  - Pèrdua o inutilització del dispositiu criptogràfic.
  - Accés no autoritzat, per un tercer, a les dades d'activació del subscriptor.
4. Circumstàncies que afecten el subscriptor o el posseïdor de claus:
  - Final de la relació entre l'EC-ACC i el subscriptor.
  - Modificació o extinció de la relació jurídica subjacent o causa que va provocar l'emissió del certificat.
  - Infracció per al sol·licitant del certificat dels requisits preestablerts per a la sol·licitud d'aquest certificat.
  - Infracció pel subscriptor de les seves obligacions, responsabilitat i garanties, establertes a l'instrument jurídic corresponent de l'EC-ACC.
  - L'extinció de la persona jurídica subscriptora del certificat, així com la finalitat de l'autorització del subscriptor al posseïdor de claus o el final de la relació entre subscriptor i posseïdor de claus.
  - Sol·licitud del subscriptor de revocació del certificat.
5. Altres circumstàncies:



- La suspensió del certificat digital per un període superior a 120 dies.
- El final del servei de l'EC-ACC, d'acord amb l'establert a la secció 9.10 d'aquesta DPC.
- Resolució judicial o administrativa que ho ordeni (art. 8.1 Llei 59/2003, de signatura electrònica)

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

L'instrument jurídic que vincula l'EC-ACC amb el subscriptor estableix que el subscriptor ha de sol·licitar la revocació del certificat en cas de tenir coneixement d'alguna de les circumstàncies indicades anteriorment.

#### 4.9.2 Legitimació per sol·licitar la revocació

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

#### 4.9.3 Procediments de sol·licitud de revocació

El procediment de revocació el duu a terme un dels operadors de l'Entitat de Registre Interna, que accedeix a l'aplicació web, mitjançant un certificat d'operador, de classe 1 o de classe 2, en funció de si és operador de l'Entitat de Registre o un operador del Centre de Trucades, emès per CATCert.

La sol·licitud de revocació ha de ser entregada personalment, enviada per correu electrònic signat o per correu certificat convencional. Ha d'incloure's la informació suficient per poder identificar raonablement, a criteri de l'EC-ACC, per una banda, el certificat que es sol·licita revocar i, d'una 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 nombre 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, registrada i notificada per l'Entitat de Registre.

S'arxiva i es comprova la documentació, s'autentica i s'autoritza el sol·licitant. En darrer lloc es realitza la revocació a la aplicació informàtica corresponent i, a continuació i de forma automàtica i immediata, s'indica la revocació en l'estat del certificat a la llista de revocacions.

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



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

#### **4.9.4 Període temporal de sol·licitud de revocació**

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

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

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

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

#### **4.9.6 Obligació de consulta d'informació de revocació de certificats**

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

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

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

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

##### **4.9.7.1 Requisits generals**

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

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

Els certificats revocats que expiren es retiren de la LRC transcorreguts seixanta dies des de l'expiració.

##### **4.9.7.2 Requisits addicionals per al Certificat CIC**

L'EC-ACC emet una LRC immediatament després de la revocació d'una Entitat de Certificació de la Jerarquia.

#### **4.9.8 Període màxim de publicació de LRCs**

Les LRC es publiquen immediatament al 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 de serveis de comprovació d'estat de certificats**

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

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

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

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

#### **4.9.11 Altres formes d'informació de revocació de certificats**

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

A la petició de consulta de vigència d'un certificat en línia s'ha de consignar un nombre de sèrie del certificat sobre el qual es realitza 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 resposta en el moment de la sol·licitud, el servei OCSP tornarà una resposta que identifiqi 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 autosignat per l'autoritat de certificació arrel de CATCert (EC-ACC)).

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

#### **4.9.12 Procediments especials en cas de compromís de la clau privada**

El compromís de la clau privada de l'EC-ACC és notificat, en la mesura possible, a tots els participants en la jerarquia pública de certificació de Catalunya, mitjançant el directori de CATCert.

### 4.9.13 Causes de suspensió de certificats

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

- Quan ho sol·liciti el subscriptor o posseïdor de claus o un tercer autoritzat (art. 9.1.a de la Llei 59/2003).
- Quan la documentació requerida a la sol·licitud de revocació sigui suficient, però no es pugui identificar raonablement el posseïdor de claus.
- Quan la documentació requerida a la sol·licitud de revocació no sigui suficient, encara que es pugui identificar raonablement el posseïdor de claus.
- Quan la documentació requerida a la sol·licitud de revocació no sigui suficient i tampoc no permeti identificar raonablement el posseïdor de claus.
- La falta d'ús del certificat durant un període prolongat de temps, conegut prèviament.
- Si se sospita el compromís d'una clau, fins que aquest sigui consignat. En aquest segon cas, l'EC-ACC s'ha d'assegurar que el certificat no està suspès durant més temps del necessari per consignar el seu compromís.
- Quan no s'activa el certificat en un termini de 120 dies a partir de la data d'emissió del certificat.

### 4.9.14 Qui pot sol·licitar la suspensió

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

### 4.9.15 Procediments de petició de suspensió

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

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

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 de que no sigui el mateix posseïdor)
- Informació de contacte de la Institució que demana la suspensió.
- Nom i cognoms del posseïdor de Claus a qui se li ha de suspendre el certificat digital.
- DNI del posseïdor de Claus a qui se li ha de suspendre el certificat digital.
- Organisme i departament al que pertany el posseïdor de Claus.
- Nombre de sèrie (serial number) del certificat digital que es sol·licita suspendre.
- Raó detallada per la petició de suspensió.
- Codi de suspensió associat al certificat o, per defecte, pregunta i resposta secreta escollida en el moment d'activar el 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 es descarregaran manualment des del directori de Certificació de CATCert instal·lades per als verificadors.

#### 4.10.2 Disponibilitat dels serveis

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

En cas d'error dels sistemes de comprovació d'estat de certificats per causes que estan fora del control de l'EC-ACC, aquesta darrera realitza els seus millors esforços per assegurar que aquest servei es mantingui inactiu el mínim temps possible. L'EC-ACC

detalla a l'apartat 5.7.4 d'aquesta DPC el temps màxim en què el servei ha de tornar a operar.

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

### **4.10.3 Altres funcions dels serveis**

Sense estipulació addicional.

## **4.11 Finalització 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**

La recuperació de claus la realitza CATCert.

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

Sense estipulació addicional.

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

L'EC-ACC s'assegura de l'aplicació dels procediments administratius i de gestió adequats conformes amb els estàndards reconeguts i, en particular:

- a. Es realitza una anàlisi de gestió de risc per avaluar les mesures necessàries de seguretat.
- b. S'és responsable per la provisió dels serveis de forma segura, fins i tot quan una part dels mateixos sigui subcontractada. Les responsabilitats de tercers es defineixen i s'han d'implantar els controls jurídics necessaris per garantir que els tercers compleixen 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 dona la publicitat necessària mitjançant accions de comunicació interna.
- d. Es manté en tot moment la infraestructura necessària per gestionar la seguretat de les operacions. Qualsevol canvi que tingui impacte en el nivell de seguretat ha de ser aprovat per l'òrgan referit al número anterior.
- e. Es documenten, implanten i mantenen els controls de seguretat i procediments d'operació de les instal·lacions, els sistemes i els actius d'informació en què se sustenta la prestació dels serveis.
- f. En cas de subcontractació total dels serveis, es garanteix el manteniment del nivell necessari de seguretat de la informació.

### 5.1 Controls de seguretat física

#### 5.1.1 Àrees segures

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

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

#### 5.1.2 Controls de seguretat física

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

- 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-ACC.

### 5.1.3 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 del moment en què se'ls notifica una incidència.

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

### 5.1.4 Accés físic

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

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

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

### 5.1.5 Electricitat i aire condicionat

Els equips informàtics de l'EC-ACC estan protegits convenientment davant de fluctuacions o talls de subministrament elèctric que puguin danyar-los o interrompre 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.



### 5.1.6 Exposició a l'aigua

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

### 5.1.7 Advertència i protecció d'incendis

Totes les instal·lacions i actius de l'EC-ACC 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 hauran de comptar amb un sistema específic i addicional a la resta de la instal·lació per a la protecció davant del foc.

### 5.1.8 Emmagatzematge de suports

L'emmagatzematge en suports d'informació es realitza de forma que es garanteix 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.

### 5.1.9 Tractament de residus

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

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

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

### 5.1.10 Còpia de seguretat fora de les instal·lacions

Periòdicament, l'EC-ACC 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'han d'adoptar mesures adients per impedir qualsevol recuperació indeguda de l'esmentada informació (com per exemple la utilització de carteres amb dispositius segurs de claus o combinacions o la utilització de fitxers xifrats).

## 5.2 Controls de procediments

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

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

### 5.2.1 Funcions fiables

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

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 d'aquesta DPC.

### 5.2.2 Nombre de persones per tasca

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

### 5.2.4 Rols que requereixen separació de tasques

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

Las funciones fiables inclouen:

- a. Oficial de Seguretat
- b. Operador de registre
- c. Administradors del sistema
- d. Operadors del sistema
- e. Auditors del sistema
- f. Cualsevol altra persona amb accés a dades de caràcter personal

Les esmentades restriccions s'apliquen en tot cas:

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

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

## 5.3 Controls de personal

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

- Es manté confidencialitat de la informació, posant els mitjans necessaris i mantenint una actitud adequada en el desenvolupament de les seves funcions i, fora de l'àmbit laboral, en allò referent a la seguretat de les infraestructures.
- S'és diligent i responsable en el tractament, el manteniment i la custòdia dels actius de la infraestructura identificats en la política, en els plans de seguretat o en aquesta 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 la seguretat de la infraestructura o limita la qualitat del servei.
- S'utilitzen els actius de la infraestructura per a les finalitats que els han estat encomanades.
- S'exigeixen manuals o guies d'usuari dels sistemes que utilitza, que permeten desenvolupar la seva funció correctament.
- S'exigeix documentació escrita que marqui les seves funcions i les mesures de seguretat a què està sotmès.
- El responsable de seguretat vetlla perquè el punt anterior sigui executat i proveeix els responsables d'àrea de tota la informació que fos necessària.
- No s'instal·la, en cap dels sistemes de la infraestructura, programari o maquinari que no sigui expressament autoritzat per escrit pel responsable de sistemes d'informació.
- No s'accedeix voluntàriament ni s'elimina o altera informació no destinada a la seva persona o perfil professional.

El personal afectat per aquesta normativa és:

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

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

- qui fa les peticions dels certificats.

- qui fa l'aprovació i la validació de les peticions de certificats.
- qui fa la generació / personalització de certificats.
- qui custodia les claus o els *tokens* criptogràfics.
- qui custodia les claus o les combinacions de seguretat d'accés a la sala d'operacions.
- qui accedeix a informació classificada.
- el personal de comunicacions i d'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-ACC l'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-ACC, especialment en relació amb procediments de personal de seguretat.

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

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

### 5.3.2 Requisits de formació

L'EC-ACC forma el personal en llocs fiables i de gestió fins que aconseguixen la qualificació necessària.

La formació inclou els continguts següents:

- Principis i mecanismes de seguretat de la jerarquia pública de certificació de Catalunya, així com l'entorn d'usuari de la persona que s'ha de formar.
- Versions de maquinari i d'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.

L'EC-ACC, 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 una instrucció periòdica en normes de seguretat, plans de contingència i gestió d'incidències.

### 5.3.3 Requisits i freqüència d'actualització formativa

Tot el personal vinculat a l'Entitat de Registre té com a requisit imprescindible l'assistència al curs de formació d'Entitats de Registre 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-ACC disposa d'un sistema sancionador per 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-ACC contracta professionals per a qualsevol funció, fins i tot per a un lloc fiable. En aquest cas, se sotmet als mateixos controls que els empleats restants.

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

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

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

### 5.3.7 Subministrament de documentació al personal

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

## 5.4 Procediments d'auditoria de seguretat

### 5.4.1 Tipus d'esdeveniments registrats

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

- L'encès i l'apagat dels sistemes.
- L'inici i la finalització de l'aplicació d'Autoritat (tècnica) de certificació.
- Els intents de crear, esborrar, canviar contrasenyes o permisos dels usuaris dins 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 de sortida del sistema.
- Els intents no autoritzats d'entrada a la xarxa de l'EC-ACC.
- Els intents no autoritzats d'accés als fitxers del sistema.
- La generació de les claus de l'EC-ACC.
- Els intents nuls de lectura i escriptura en un certificat i en el directori.
- Esdeveniments relacionat amb el cicle de vida del certificat, com una sol·licitud, una emissió, una revocació i una renovació d'un certificat.
- Esdeveniments relacionat amb el cicle de vida del mòdul criptogràfic, com recepció, ús i desinstal·lació d'aquest.

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

- 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-ACC.
- 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 almenys una vegada a la setmana per tal de cercar activitat sospitosa o no habitual.

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

### 5.4.3 Període de conservació de registres d'auditoria

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

#### 5.4.4 Protecció dels registres d'auditoria

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

#### 5.4.5 Procediments de còpia de seguretat

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

Per tal de conservar correctament les còpies de seguretat realitzades, l'EC-ACC té adoptades, com a mínim, les mesures de seguretat següents:

- S'emmagatzemen 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 (disquetes, DVD's...) i es volen reutilitzar s'assegura que les dades que ha contingut estiguin completament esborrats fent impossible la seva recuperació.
- S'autoritza expressament l'extracció de les còpies de seguretat fora de l'Entitat de Registre, omplint una fitxa al respecte i anotant el corresponent detall en un llibre de registre.
- Es procura anar depositant còpies de seguretat periòdicament fora de l'Entitat de Registre.

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

El sistema d'acumulació de registres d'auditoria és, almenys, un sistema intern de l'EC-ACC, compost pels registres de l'aplicació, pels registres de xarxa, pels registres del sistema operatiu i per les dades manualment generades, que emmagatzemarà el 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 es guarden, en part, per monitoritzar les vulnerabilitats del sistema.



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

Aquestes anàlisis s'executen diàriament, mensualment i anualment d'acord amb la seva definició en el Pla d'Auditoria de l'EC-ACC.

## 5.5 Arxiu d'informacions

L'EC-ACC garanteix que tota la informació relativa als certificats es guarda durant un període de temps apropiat, segons l'establert a la secció 5.5.2 d'aquesta DPC.

### 5.5.1 Tipus d'esdeveniments registrats

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

L'EC-ACC guarda un registre del següent:

Documents originals:

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

### 5.5.2 Període de conservació de registres

#### 5.5.2.1 Requisits per a tots els tipus de certificats

L'EC-ACC guarda els registres especificats a la secció 5.5.1 d'aquesta DPC durant 5 anys, comptats des del moment de l'expedició del certificat. Tota la informació relativa als Certificats d'Infraestructura de Certificació es guarda de forma permanent.

#### 5.5.2.2 Requisits específics per als certificats CIPIR

No obstant allò que es disposa a la secció 5.2.2.1 anterior, l'EC-ACC guarda els registres dels certificats CIPIR durant 15 anys, a comptar des del moment de l'expedició d'aquests.

### 5.5.3 Protecció de l'arxiu

L'EC-ACC:

- 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 seguretat

Un tècnic de comunicacions de l'EC-ACC s'encarrega de fer i de verificar la realització de les còpies de seguretat dels *logs* d'accés lògic al sistema operatiu de la LRA.

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

També es realitzen còpies de seguretat de l'aplicació KeyOne personalitzada per a l'EC-ACC. CATCert guarda aquestes còpies a les seves instal·lacions.

#### 5.5.5 Requisits de segellat de cautela de data i hora

L'EC-ACC emet els certificats i les LRC amb informació de temps i hora.

#### 5.5.6 Localització del sistema d'arxiu

L'EC-ACC té un sistema de manteniment de dades d'arxiu fora de les seves pròpies instal·lacions, així com s'especifica a la secció 5.1.10 d'aquesta DPC.

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

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

### 5.6 Renovació de claus

Els certificats de l'EC-ACC que s'hagin renovat, es comuniquen als usuaris finals, mitjançant la seva publicació al directori de CATCert.

### 5.7 Compromís de claus i recuperació de desastre

#### 5.7.1 Procediment de gestió d'incidències i compromisos

L'EC-ACC estableix els procediments que aplica a la gestió de les incidències que afecten les seves claus i, molt especialment, als 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-ACC inicia les gestions necessàries, segons els documents Pla de Seguretat, Pla d'Emergència i Pla d'Auditoria, per fer que el sistema torni al seu estat normal de funcionament.

#### 5.7.3 Compromís de la clau privada de l'Entitat

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

En cas de compromís, l'EC-ACC:

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

#### 5.7.4 Desastre sobre les instal·lacions

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

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

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

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

### 5.8 Finalització del servei

#### 5.8.1 EC-ACC

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

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

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

L'EC-ACC declara a les seves pràctiques les previsions que ha d'adoptar en cas de finalització del servei. Aquestes inclouen:

- 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-ACC a altres persones, sota el seu consentiment..
- Com es tracta l'estat de revocació dels certificats emesos que encara no han expirat.

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

### 5.8.2 Entitat de Registre

Sense estipulació addicional.

## 6. Controls de seguretat tècnica

L'EC-ACC utilitza sistemes i productes fiables que estan protegits contra tot tipus d'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

Les claus pública i privada dels certificats podran ser generades pel futur subscriptor o per l'EC-ACC.

#### 6.1.2 Enviament de la clau privada al subscriptor

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

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

El mètode d'enviament de la clau pública a l'EC-ACC és PKCS #10, una 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-ACC i les claus de les Entitats de Certificació anteriors en la jerarquia pública de certificació de Catalunya es comuniquen als verificadors, i així s'assegura la integritat de la clau i se n'autentica l'origen.

La clau pública de l'EC-ACC (Entitat de Certificació de l'Agència Catalana de Certificació-CATCert), que és l'arrel de la jerarquia, es publica al directori de l'EC-ACC en forma de certificat auto-signat juntament amb una declaració que fa referència al fet que la clau permet autenticar a l'EC-ACC.

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

La clau pública de l'EC-ACC es publica al directori de l'EC-ACC en forma de certificat CIC signat per CATCert.

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

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

### 6.1.5 Mesures de claus

Les claus de l'EC-ACC són almenys de 2.048 bits.

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

### 6.1.6 Generació de paràmetres de clau pública

Sense estipulació addicional.

### 6.1.7 Comprovació de qualitat de paràmetres de clau pública

Es realitza d'acord amb l'especificació tècnica de l'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-ACC són generats utilitzant maquinari criptogràfic que compleix els requisits establerts per l'especificació tècnica CEN CWA 141617 o equivalent.

Els parells de claus dels subscriptors de certificats CIPIR s'han de generar 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.

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

### 6.1.9 Propòsits d'ús de claus

L'EC-ACC inclou l'extensió Key Usage en tots els certificats, que indica els usos permesos de les corresponents claus privades.

L'extensió Key Usage s'utilitza per establir límits tècnics als usos que es pugui donar a una clau privada corresponent a una clau pública llistada en un certificat X.509v3. Cal tenir en compte 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 ser controlades per CATCert.

## 6.2 Protecció de la clau privada

### 6.2.1 Estàndards de mòduls criptogràfics

#### 6.2.1.1 Estàndards dels mòduls criptogràfics

Les claus privades de les Entitats de Certificació 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 CIPISR estan protegits per targetes intel·ligents 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 (també targetes intel·ligents) es lliuren en cada emissió de nou certificat per l'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 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 cas puntuals, es substituirà la targeta afectada, prèvia revocació del certificat i s'emetrà un nou certificat que es lliurarà en una targeta nova sense cost addicional per al subscriptor.

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

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

Cadascun 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 persona no coneix més d'una de les claus d'accés.

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

#### **6.2.3 Dipòsit de la clau privada**

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

#### **6.2.4 Còpia de seguretat de la clau privada**

Existeix una còpia de seguretat de la clau privada de l'EC-ACC i dels mitjans necessaris per accedir en un lloc independent d'aquell on s'emmagatzema habitualment.

#### **6.2.5 Arxiu de la clau privada**

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

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

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



### 6.2.6 Introducció de la clau privada en el mòdul criptogràfic

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

Aquestes targetes s'utilitzen per introduir la clau privada en el mòdul criptogràfic.

### 6.2.7 Emmagatzematge de la clau privada en el mòdul criptogràfic

Les claus privades es generen directament en els mòduls criptogràfics.

### 6.2.8 Mètode d'activació de la clau privada

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

Per a certificats CIPISR, 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

Per a certificats CIPISR, quan la targeta intel·ligent o dispositiu criptogràfic es retiri del dispositiu lector, serà necessària novament la introducció del PIN.

### 6.2.10 Mètode de destrucció de la clau privada

Les claus privades són destruïdes de forma que impedeixi el seu robatori, modificació, divulgació o ús no autoritzat.

### 6.2.11 Classificació dels mòduls criptogràfics

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

Els mòduls dels subscriptors de certificats CIPISR obtenen o superen el nivell EAL 4 de Common Criteria (ISO 15408) amb els augments que es determinen a l'especificació tècnica CEN CWA 14169.

## 6.3 Altres aspectes de gestió del parell de claus

### 6.3.1 Arxiu de la clau pública

L'EC-ACC arxiva les seves claus públiques, d'acord amb l'establert a la secció 5.5 d'aquesta DPC.

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

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

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

## 6.4 Dades d'activació

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

L'EC-ACC facilita al subscriptor, per una banda, les dades d'activació de la targeta i, al cap de 3 dies, la targeta.

### 6.4.2 Protecció de dades d'activació

#### 6.4.2.1 Per a certificats CIPSR

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

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

- L'EC-ACC garanteix que l'accés als sistemes d'informació i aplicacions es restringeix d'acord a l'establert a la política de control d'accés, així com que els sistemes proporcionen els controls de seguretat suficients per implementar la segregació de funcions identificada a les pràctiques de l'EC-ACC, 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-ACC s'identifica i es reconeix abans d'utilitzar aplicacions crítiques relacionades amb el cicle de vida del certificat.
- El personal de l'EC-ACC 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 quedin accessibles a usuaris no autoritzats.
- Els sistemes de seguretat i monitoratge permeten una ràpida detecció, registre i actuació davant d'intents d'accessos irregulars o no autoritzats als seus recursos (per exemple, mitjançant un sistema de detecció d'intrusions, monitoratge i alarma).
- L'accés als directoris públics de la informació de l'EC-ACC (per exemple, certificats o informació d'estat de revocació) compta amb un control d'accessos per a modificacions o esborrament de dades.

## 6.5.2 Avaluació del nivell de seguretat informàtica

Les aplicacions de EC i ER són fiables, d'acord amb l'especificació tècnica CEN CWA 14167-1, i s'avalua el grau de compliment mitjançant una auditoria de seguretat informàtica conforme a l'especificació tècnica CWA 14172-2 i un perfil de protecció adient, 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 garantir que els sistemes són segurs.

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

### 6.6.2 Controls de gestió de seguretat

L'EC-ACC 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 fallida dels sistemes.

- c. Protegir els mòduls contra virus i software maliciós, per garantir la integritat i validesa de la informació que processen.

L'EC-ACC manté un inventari de tots els actius informàtics i en realitza una classificació d'acord amb les seves necessitats de protecció i coherent amb l'anàlisi de riscos efectuada.

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

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

### 6.6.3 Avaluació del nivell de seguretat del cicle de vida

Sense estipulació addicional.

## 6.7 Controls de seguretat de xarxa

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

- S'implementen controls (com, per exemple, tallafocs) per protegir la xarxa interna de dominis externs accessibles per terceres parts. Els tallafocs es configuren de forma que s'impedeixin accessos i protocols que no siguin necessaris per a l'operació de l'EC-ACC.
- Les dades sensibles es protegeixen quan s'intercanvien a través de xarxes no segures (incloent les dades de registre del subscriptor).
- Es garanteix que els components locals de xarxa (com encaminadors) es troben ubicats en entorns segurs, així com l'auditoria periòdica de les seves configuracions.

## 6.8 Segell de temps

Sense estipulació addicional.

## 7. Perfils de certificats i llistes de certificats revocats

---

### 7.1 Perfil de certificat

Aquesta secció es troba al web ([www.catcert.net/registre](http://www.catcert.net/registre)).

### 7.2 Perfil de la llista de revocació de certificats

Aquesta secció es troba al web ([www.catcert.net/registre](http://www.catcert.net/registre)).

## 8. Auditoria de conformitat

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

A part de l'auditoria de conformitat, l'EC-ACC realitza altres revisions de caràcter puntual per demostrar la seva confiança. D'aquesta manera, quan s'accepta una nova Entitat de Certificació subordinada a la jerarquia, es realitza una revisió dels documents de seguretat, DPC i PdC de CATCert per assegurar que compleix els requisits de seguretat i d'operació necessaris per formar part de la Jerarquia d'Entitats de Certificació de CATCert.

Així mateix, si se sospita que una Entitat de Certificació en funcionament no compleix algun dels requisits de seguretat o si s'ha detectat un compromís de claus o qualsevol esdeveniment que pugui suposar un perill per a la seguretat o la integritat de l'Entitat de Certificació Vinculada, es durà a terme una auditoria interna.

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

### 8.1 Freqüència de l'auditoria de conformitat

L'EC-ACC duu a terme anualment una auditoria de conformitat, 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 es pot encarregar, a través del seu departament d'auditoria, de realitzar l'auditoria de conformitat.

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

### 8.3 Relació de l'auditor amb l'entitat auditada

Les auditories de conformitat executades per tercers les realitzarà una entitat independent de l'EC-ACC auditada. En cas d'auditoria interna l'EC-ACC s'ha d'assegurar que no existeix conflicte d'interessos que afecti negativament a 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 manca de conformitat

Una cop rebut l'informe de l'auditoria de compliment dut a terme, l'EC-ACC discuteix, amb l'entitat que ha executat l'auditoria i amb CATCert, les deficiències trobades i desenvolupa i executa un pla correctiu que les soluciona.

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

- Revocar la clau de l'EC-ACC, tal com es descriu a la secció 4.9 d'aquesta DPC.
- Acabar el servei de l'EC-ACC, tal com es descriu a la secció 5.8 d'aquesta DPC.

## 8.6 Tractament dels informes d'auditoria

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



## 9. Requisits comercials i legals

---

### 9.1 Tarifes

#### 9.1.1 Tarifa d'emissió o renovació de certificats

CATCert estableix les tarifes que aplica l'EC-ACC, en la prestació dels seus serveis. Las tarifas se pueden consultar en la web de CATCert (<http://www.catcert.cat/tarifas/>).

#### 9.1.2 Tarifa d'accés a certificats

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

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

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

#### 9.1.4 Tarifes d'altres serveis

Sense estipulació addicional

#### 9.1.5 Política de reintegrament

CATCert no practicarà reintegraments. En cas de productes defectuosos es procedirà a substituir el producte defectuós per un 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, de signatura electrònica. Aquesta assegurança cobreix les actuacions de CATCert com a prestador de serveis de certificació.

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

#### 9.2.2 Altres actius

Sense estipulació addicional.

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

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

## 9.3 Confidencialitat

### 9.3.1 Informacions confidencials

Les informacions següents es mantenen de forma confidencial per l'EC-ACC:

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

### 9.3.2 Informacions no confidencials

Les informacions següents no tenen caràcter confidencial:

- Aquesta Declaració de Pràctiques de Certificació de l'EC-ACC.
- Qualsevol altra informació identificada com a "Pública".

### 9.3.3 Responsabilitat per a la protecció d'informació confidencial

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

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

## 9.4 Protecció de dades personals

### 9.4.1. Política de Protecció de Dades Personals

CATCert desenvolupa una política de protecció de les dades personals, d'acord amb la Llei Orgànica 15/99, de 13 de desembre, de Protecció de Dades de Caràcter Personal (LOPD) i la normativa reglamentària 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 6.1.
- b. Mesures, normes, procediments, regles i estàndards que garanteixin el nivell de seguretat exigít pel RD 1720/2007 - secció 6.1, i, en general, tots els controls tècnics de les seccions 5 i 6 de la Política General de Certificació de CATCert.
- 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

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

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

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

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

### 9.5.2 Propietat de la política de certificat i Declaració de Pràctiques de Certificació

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

L'EC-ACC és propietària d'aquesta DPC.

### 9.5.3 Propietat de la informació relativa a noms

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

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

#### 9.6.1.1 Obligacions i altres compromisos

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

- Determina la comunitat de subscriptors i verificadors de l'EC-ACC.
- 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-ACC, d'acord amb el procediment previst en aquesta Declaració de Pràctiques de Certificació.
- Informa puntualment CATCert de totes les informacions relatives als canvis a realitzar, incidències en el servei, reclamacions, denúncies i inspeccions del servei.
- Garanteix, sota la seva plena responsabilitat, que compleix amb tots els requisits establerts en aquesta DPC.
- És l'única entitat responsable del compliment dels procediments descrits en aquesta DPC, fins i tot quan una part o la totalitat de les operacions siguin subcontractades externament.
- Presta els seus serveis de certificació d'acord amb aquesta DPC, on es detallen, almenys, els continguts previstos a l'article 19 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.
- Abans de l'emissió i lliurament del certificat, l'EC-ACC informa dels aspectes previstos a l'article 18. b) de la Llei 59/2003, de 19 de desembre, de signatura electrònica, així com dels següents aspectes:
  - Indicació de la política aplicable, amb indicació que els certificats no s'expedeixen al públic i la necessitat d'utilització de dispositiu segur de creació de signatura.
  - Forma en què es garanteix la responsabilitat patrimonial de l'EC-ACC.
  - L'EC-ACC es declara d'acord amb la política de certificació, la certificació del prestador de serveis de certificació i la certificació dels productes de signatura electrònica utilitzats.

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

- L'EC-ACC obliga als subscriptors, posseïdors de claus i als verificadors mitjançant instruments jurídics apropiats en cada situació, els quals es transmeten electrònicament, en llenguatge escrit i comprensible, a tenir en compte els continguts mínims següents:
  - Prescripcions per donar compliment a l'establert en aquesta DPC.

- 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 al 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 l'esmentada informació en tercers, en cas de final d'operacions de l'EC-ACC sense revocació de certificats vàlids.
  - Límits d'ús del certificat, incloent els establerts a la secció 4.5 d'aquesta DPC.
  - 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-ACC accepta o exclou la seva responsabilitat.
  - Procediments aplicables de resolució de disputes.
  - Llei aplicable i jurisdicció competent.
- L'EC-ACC identifica el posseïdor de claus, d'acord amb els articles 12 i 13 de la Llei 59/2003, de 19 de desembre, de signatura electrònica i aquesta DPC. Especialment, l'EC-ACC, comprova per si mateixa la identitat i altres circumstàncies personals dels sol·licitants dels certificats, d'acord amb l'establert a l'article 13 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

#### 9.6.1.2 Garanties ofertes

- Garanties ofertes als subscriptors

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

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.

Que no hi ha errors en les informacions contingudes als certificats, coneguts o realitzats per aquesta, ni deguts a la manca de diligència en la gestió de la sol·licitud de certificat o en la creació d'aquest.

Que els certificats compleixen tots els requisits materials establerts a la DPC.

Que els serveis de revocació i l'ús del directori compleixen tots els requisits materials establerts a la DPC.

- a) Que, en cas que hagi generat les claus privades, es manté la confidencialitat durant el procés.

- b) La responsabilitat de l'EC-ACC, amb els límits que s'estableixin.

## Garanties ofertes als verificadors

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

- 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, de signatura electrònica.
- Que la informació continguda o incorporada per referència al certificat és correcta, excepte quan indiqui expressament el contrari.
- En cas de certificats publicats al 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 d'aquesta DPC.
- 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 aquesta DPC.
- La rapidesa i seguretat en la prestació dels serveis, en especial dels serveis de revocació i de directori.
- Que els certificats compleixin tots els requisits materials establerts en aquesta DPC.
- Que, en cas que hagi generat les claus privades, es manté la confidencialitat durant el procés.
- Que els serveis de revocació i l'ús del directori compleixen tots els requisits materials establerts en aquesta DPC.
- La responsabilitat de l'EC-ACC, amb els límits que s'estableixin.

## 9.6.2 Entitats de Registre

### 9.6.2.1 Obligacions i altres compromisos

#### Entitats de Registre

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

- Actua exclusivament en relació amb persones vinculades a l'Entitat de Registre.
- Nomena com a operador de l'autoritat de registre, a un o més dels seus treballadors, i comunica a CATCert les dades corresponents a aquestes persones per a l'emissió dels certificats d'operador corresponent. Quan un operador deixa de tenir capacitat per actuar com el que és, sota el control i l'autoritat de l'Entitat de Registre, aquesta Entitat sol·licita de forma immediata a l'EC-ACC la revocació del certificat d'operador corresponent.
- Valida i aprova les sol·licituds de certificats i, tot seguit, genera les targetes per als posseïdors de claus, d'acord amb els procediments i instruments tècnics establerts per l'EC-ACC, d'acord amb aquesta DPC i la seva documentació d'operacions.
- Si l'Entitat de Registre Interna no disposa d'informació actualitzada del posseïdor de claus, comprova la identitat personalment o d'acord amb l'establert a l'article 13.4 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, registra un

justificant acreditatiu del nom complet, lloc i data de naixement, DNI i/o qualsevol altra informació que pugui ser utilitzada per diferenciar una persona respecte d'una altra en l'àmbit de l'Entitat de Registre Interna.

- e. Verifica, quan sigui necessari, qualsevol atribut específic del posseïdor de claus, i registra un justificant acreditatiu de la informació.
- f. Realitza o tramita les sol·licituds de suspensió, reactivació, revocació i renovació de certificats, d'acord amb els procediments i els instruments tècnics establerts per l'EC-ACC, d'acord amb aquesta DPC, i la seva documentació d'operacions.
- g. Emmagatzema els registres, ja sigui en paper o de forma electrònica, amb les mesures adequades de seguretat, autenticitat, integritat i conservació, relatives a la informació continguda al certificat, durant un període de 15 anys. Aquests registres estan a disposició de l'EC-ACC.

### 9.6.3 Subscriptors

#### 9.6.3.1 Obligacions i altres compromisos

##### *Requisits per a tots els tipus de certificats*

L'EC-ACC obliga al subscriptor dels certificats a:

- a. Facilitar a l'EC-ACC la informació completa i adequada conforme als requeriments d'aquesta DPC, en especial, en allò referent al procediment de registre.
- b. Manifestar el seu consentiment previ a l'emissió i lliurament d'un certificat.
- c. Complir les obligacions que s'estableixen per al subscriptor en aquesta 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 l'establert a la secció 1.4 d'aquesta DPC.
- e. Notificar a l'EC-ACC, sense retards 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-ACC i a qualsevol persona que el subscriptor cregui que pugui confiar en el certificat sense retards injustificables:
  - a La pèrdua, el robatori o el compromís potencial de la seva clau privada.
  - b La pèrdua de control sobre la seva clau privada, a causa del compromís de les dades d'activació (per exemple, el codi PIN del dispositiu segur de creació de signatura) o per qualsevol altra causa.
  - c Les inexactituds o canvis en el contingut del certificat que conegui o pogués conèixer el subscriptor.
- g. Deixar d'utilitzar la clau privada un cop 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 reversa 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.

#### 9.6.3.2 Garanties ofertes pel subscriptor

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

- a. Totes les manifestacions realitzades a la sol·licitud són correctes.
- b. Totes les informacions subministrades pel subscriptor que es trobin contingudes al certificat són correctes.
- c. El certificat s'utilitza exclusivament per a usos legals i autoritzats, d'acord amb aquesta DPC.
- d. Cada signatura digital creada amb la clau privada corresponent a la clau pública llistada al certificat és la signatura digital del subscriptor i que el certificat ha estat acceptat i es troba operatiu (no ha expirat ni ha estat revocat) en el moment de creació de la signatura.
- e. El subscriptor és una entitat final i no una Entitat de Certificació i no utilitza la clau privada corresponent a la clau pública llistada al certificat per signar cap certificat (o qualsevol altre format de clau pública certificada) ni LRC.
- f. Cap persona no autoritzada no ha tingut mai accés a la clau privada del subscriptor.

#### 9.6.3.3 Protecció de la clau privada

L'EC-ACC s'obliga, 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-ACC 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 a 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 que es trobi al mateix certificat o en el contracte de verificador.
- e. Tenir present qualsevol precaució establerta en un contracte o en un altre instrument, amb independència de la seva naturalesa jurídica.

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

#### 9.6.4.2 Garanties ofertes pel verificador

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

- a. Disposa de suficient informació per prendre una decisió informada per confiar o no en el certificat.
- b. És l'únic responsable de confiar o no en la informació continguda al certificat.
- c. Serà l'únic responsable si incompleix les seves obligacions com a verificador.

### 9.6.5 CATCert

#### 9.6.5.1 Obligacions i compromisos

CATCert té les obligacions següents:

- a. Operar l'EC-ACC, Entitat de certificació arrel de la jerarquia pública de certificació de Catalunya, de manera diligent, de conformitat amb les polítiques, pràctiques i normativa de l'esmentada jerarquia.
- b. Operar les seves Entitats de Certificació Vinculades, pròpies o que prestin serveis a les Entitats de Certificació Virtuals, d'acord amb allò que es disposa a la Política General de Certificació.
- c. Garantir l'equivalència de la seguretat de l'operació de les Entitats de Certificació Vinculades de tercers prestadors de serveis de certificació i, especialment, vetllar perquè aquests compleixin amb les obligacions previstes a la Política General de Certificació.

#### 9.6.5.2 Garanties ofertes als subscriptors

CATCert garanteix que la clau privada de l'EC-ACC no ha estat compromesa, llevat que així ho indiqui expressament mitjançant el directori de CATCert.

CATCert únicament garanteix:

- a. Que els certificats contenen tota la informació exigida per la Llei 59/2003, de 19 de desembre, de signatura electrònica.
- b. Que no ha originat ni introduït declaracions falses o errònies a la informació dels certificats, ni tampoc ha deixat d'incloure informació necessària aportada per l'EC-

ACC i validada per CATCert o l'Entitat de Registre, en el moment d'emissió dels certificats.

- c. Que tots els certificats emesos compleixen els requisits formals i de contingut.

CATCert està vinculada als procediments operatius i de seguretat descrits en aquesta DPC.

### 9.6.5.3 Garanties ofertes als verificadors

La responsabilitat de CATCert, que deriva d'una relació indirecta, és la prevista a l'article 23.4 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

### 9.6.5.4 Exclusió de garanties

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

## 9.6.6 Directori

### 9.6.6.1 Obligacions i compromisos

L'EC-ACC pot delegar algunes funcions al 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 en aquesta DPC, així com en la documentació jurídica auxiliar, especialment la lliurada a subscriptors, posseïdors de claus i verificadors.

### 9.6.6.2 Garanties

L'EC-ACC estableix en aquesta 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-ACC

L'EC-ACC 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-ACC

L'EC-ACC 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) subministrats per aquesta.

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

### 9.8.2 Cas fortuït i força major

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

## 9.9 Indemnitzacions

### 9.9.1 Clàusula d'indemnitat de subscriptor

No s'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-ACC estableix, als seus instruments jurídics amb els subscriptors i els verificadors, una clàusula que determina el període de vigència de la relació jurídica en virtut de la qual subministra certificats als subscriptors.

### 9.10.2 Finalització

L'EC-ACC estableix, als 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 subministra certificats als subscriptors.

### 9.10.3 Supervivència

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

A aquest efecte, l'EC-ACC vetlla perquè, almenys els requisits continguts a les seccions Obligacions, Responsabilitat civil, Auditoria de conformitat i Confidencialitat, continuïn vigents després de la finalització de la política de certificació i dels instruments jurídics que vinculin l'EC-ACC amb subscriptors i verificadors.

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

## 9.11 Notificacions

L'EC-ACC estableix, als seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules de notificació, en les quals s'estableix el procediment pel qual les parts es notifiquen fets mútuament.

## 9.12 Modificacions

### 9.12.1 Procediment per a les modificacions

L'EC-ACC pot modificar, de forma unilateral, aquesta DPC, sempre que procedeixi segons el procediment següent:

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

### 9.12.2 Període i mecanismes per a notificacions

Les modificacions d'aquesta DPC es notifiquen a CATCert, per a la seva posterior aprovació.

### 9.12.3 Circumstàncies en les quals un OID s'ha de canviar

Sense estipulació addicional.

## 9.13 Resolució de conflictes

### 9.13.1 Resolució extrajudicial de conflictes

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

Amb aquesta finalitat, es té en compte la consideració com a Administració Pública de l'EC-ACC.

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

### 9.13.2 Jurisdicció competent

L'EC-ACC estableix, als seus instruments jurídics vinculants amb subscriptors i verificadors, una clàusula de jurisdicció competent, que indica que la competència judicial internacional correspon als jutges espanyols.

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

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

## 9.14 Llei aplicable

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

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

## 9.15 Conformitat amb la llei aplicable

L'EC-ACC manifesta el compliment de la Llei 59/2003, de 19 de desembre, de signatura electrònica, en aquesta DPC.

## 9.16 Clàusules diverses

### 9.16.1 Acord íntegre

L'EC-ACC estableix, als seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules d'acord íntegre, en virtut de les quals s'entén que l'instrument jurídic regulador del servei conté la voluntat completa i tots els acords entre les parts.

### 9.16.2 Subrogació

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

En cas que es produeixi una cessió o subrogació, es procedeix a la finalització de l'esmentada Entitat de Certificació.

### 9.16.3 Divisibilitat

L'EC-ACC estableix clàusules de divisibilitat, als seus instruments jurídics vinculants amb subscriptors i verificadors, en virtut de les quals la invalidesa d'una clàusula no afecta la resta del contracte.

Donat cas que, com a causa als articles 7 i 8 de la Llei 7/1998 sobre condicions generals de la contractació, es consideressin 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.

## ANNEX I

### Control documental

Projecte:	<b>Informe modificació del document DPC EC-ACC</b>
Entitat de destí:	<b>Agència Catalana de Certificació</b>
Codi de referència:	<b>Revisió 1r semestre 2011</b>
Versió:	<b>Canvis de la v1.1 a la 1.2 en català i en castellà</b>
Data de l'edició:	<b>31/06/2010</b>

### Control de versions DPC EC-ACC 1r semestre 2011

Versió	Parts que canvien	Descripció del canvi	Autor del canvi	Data del canvi
1.2	4.8	Nou redactat per a la modificació de certificats	Oficina de polítiques	30/06/2011
1.2	5.8.1	Modificació de les condicions per la finalització del servei	Oficina de Polítiques	30/06/2011
1.2	6.1.5	Actualització mida claus	Oficina de Polítiques	30/06/2011
1.2	6.4.2.1	Adaptació del procediment de lliurament al refactoring	Oficina de Polítiques	30/06/2011
1.2	9.6	Reestructuració de la informació relativa a les obligacions de l'EC i les ER	Oficina de Polítiques	30/06/2011