



**Agència Catalana  
de Certificació**

---


**Política General de Certificació  
Agència Catalana de Certificació**

Referència: D1111\_E0650\_N-PGdC  
Versió: 3.6  
Data: 03/11/2011

---

## Control documental

---

<b>Estat formal</b>	<b>Elaborat per:</b>  (Àrea d'Assessorament)	<b>Aprovat per:</b>  Marta Cruellas
<b>Data de creació</b>	27/08/2007	
<b>Control de versions</b>	<b>Data:</b>	03/11/2011
	<b>Descripció:</b>	Annex I
<b>Nivell accés informació</b>	pública	
<b>Títol</b>	Política General de Certificació v3r6 cat	
<b>Fitxer</b>	D1111 E0650 N-PGdC v3r6 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>	

<b>1. Introducció.....</b>	<b>11</b>
1.1 PRESENTACIÓ .....	12
1.1.1 Tipus i classes de certificats .....	12
1.1.2 Relació entre la política de certificació i altres documents .....	17
1.1.3 Termes habituals utilitzats en aquest document .....	17
1.2 NOM DEL DOCUMENT I IDENTIFICACIÓ.....	20
1.3 COMUNITAT D'USUARIS DE CERTIFICATS .....	21
1.3.1 Prestadors de serveis de certificació .....	21
1.3.2 Entitat de Certificació Arrel .....	22
1.3.3 Entitats de Certificació Vinculades.....	22
1.3.4 Entitats de Registre .....	23
1.3.5 Usuaris finals.....	23
1.4 ÚS DELS CERTIFICATS.....	25
1.4.1 Usos típics del certificats .....	25
1.4.2 Aplicacions prohibides.....	30
1.5 ADMINISTRACIÓ DE LA POLÍTICA .....	33
1.5.1 Organització que administra l'especificació .....	33
1.5.2 Dades de contacte de l'organització .....	33
1.5.3 Persona que determina la conformitat d'una DPC amb la política .....	33
1.5.4 Procediment d'aprovació .....	34
<b>2. Publicació d'informació i directori de certificats.....</b>	<b>35</b>
2.1 DIRECTORI DE CERTIFICATS .....	35
2.2 PUBLICACIÓ D'INFORMACIÓ DE L'ENTITAT DE CERTIFICACIÓ .....	35
2.3 FREQUÈNCIA DE PUBLICACIÓ .....	35
2.4 CONTROL D'ACCÉS.....	36
<b>3. Identificació i autenticació.....</b>	<b>37</b>
3.1 GESTIÓ DE NOMS .....	37
3.1.1 Tipus de noms.....	37
3.1.2 Significat dels noms .....	37
3.1.3 Utilització d'anònims i pseudònims .....	37
3.1.4 Interpretació de formats de noms .....	37
3.1.5 Unicitat dels noms .....	38
3.1.6 Resolució de conflictes relatius a noms.....	38
3.2 VALIDACIÓ INICIAL DE LA IDENTITAT .....	41
3.2.1 Prova de possessió de clau privada .....	41
3.2.2 Autenticació de la identitat d'una organització .....	41

3.2.3	Autenticació de la identitat d'una persona física .....	43
3.2.4	Informació de subscriptor no verificada .....	45
3.3	IDENTIFICACIÓ I AUTENTICACIÓ DE SOL·LICITUDS DE RENOVACIÓ .....	45
3.3.1	Validació per a la renovació rutinària de certificats .....	45
3.3.2	Validació per a la renovació de certificats després de la revocació.....	46
3.4	IDENTIFICACIÓ I AUTENTICACIÓ DE LA SOL·LICITUD DE REVOCACIÓ .....	46
3.5	AUTENTICACIÓ D'UNA PETICIÓ DE SUSPENSIO .....	46
<b>4.</b>	<b>Característiques d'operació del cicle de vida dels certificats .....</b>	<b>47</b>
4.1	SOL·LICITUD D'EMISSIÓ DE CERTIFICAT .....	47
4.1.1	Legitimació per sol·licitar l'emissió .....	47
4.1.2	Procediment d'alta; Responsabilitats .....	49
4.2	PROCESSAMENT DE LA SOL·LICITUD DE CERTIFICACIÓ .....	49
4.2.1	Requisits per a tots els tipus de certificats .....	49
4.2.2	Requisits específics per al CIC .....	49
4.2.3	Requisits per als certificats personals.....	50
4.2.4	Requisits per als certificats d'entitat.....	51
4.2.5	Requisits per als certificats de dispositiu .....	52
4.3	EMISSIÓ DE CERTIFICAT.....	52
4.3.1	Accions de l'Entitat de Certificació durant el procés d'emissió .....	52
4.3.2	Notificació de l'emissió al subscriptor .....	53
4.4	ACEPTACIÓ DEL CERTIFICAT .....	54
4.4.1	Responsabilitats del Prestador de Serveis de Certificació .....	54
4.4.2	Conducta que constitueix acceptació del certificat.....	54
4.4.3	Publicació del certificat .....	55
4.4.4	Notificació de l'emissió a tercers.....	55
4.5	ÚS DEL PARELL DE CLAUS I DEL CERTIFICAT .....	55
4.5.1	Ús pels subscriptors .....	55
4.5.2	Ús pel tercer que confia en certificats.....	56
4.6	RENOVACIÓ DE CERTIFICATS SENSE RENOVACIÓ DE CLAUS .....	56
4.6.1	Requisits específics per als certificats d'infraestructura .....	56
4.6.2	Requisits específics per als certificats de signatura electrònica reconeguda .....	56
4.6.3	Requisits específics per a la resta de certificats personals .....	57
4.7	RENOVACIÓ DE CERTIFICAT AMB RENOVACIÓ DE CLAUS .....	57
4.8	RENOVACIÓ TELEMÀTICA .....	57
4.9	MODIFICACIÓ DE CERTIFICATS .....	57
4.10	REVOCACIÓ I SUSPENSIO DE CERTIFICATS.....	58

4.10.1	Causes de revocació de certificats .....	58
4.10.2	Legitimació per sol·licitar la revocació .....	60
4.10.3	Procediments de sol·licitud de revocació .....	60
4.10.4	Termini temporal de sol·licitud de revocació .....	61
4.10.5	Termini màxim de processament de la sol·licitud de revocació.....	61
4.10.6	Obligació de consulta d'informació de revocació de certificats .....	61
4.10.7	Freqüència d'emissió de llistes de revocació de certificats (LRCs) .....	62
4.10.8	Període màxim de publicació de LRCs.....	62
4.10.9	Disponibilitat de serveis de comprovació d'estat de certificats .....	62
4.10.10	Obligació de consulta de serveis de comprovació d'estat de certificats.....	63
4.10.11	Altres formes d'informació de revocació de certificats .....	63
4.10.12	Requeriments especials en cas de compromís de la clau privada .....	63
4.10.13	Causes de suspensió de certificats.....	63
4.10.14	Qui pot sol·licitar la suspensió.....	63
4.10.15	Procediments de petició de suspensió .....	64
4.10.16	Termini màxim de suspensió .....	64
4.10.17	Habilitació d'un certificat suspès .....	64
4.11	SERVEIS DE COMPROVACIÓ D'ESTAT DE CERTIFICATS .....	64
4.11.1	Característiques d'operació dels serveis .....	64
4.11.2	Disponibilitat dels serveis .....	64
4.11.3	Altres funcions dels serveis .....	65
4.12	FINALITZACIÓ DE LA SUBSCRIPCIÓ.....	65
4.13	DIPÒSIT I RECUPERACIÓ DE CLAUS.....	65
4.13.1	Política i pràctiques de dipòsit i recuperació de claus.....	65
4.13.2	Política i pràctiques d'encapsulament i recuperació de claus de sessió.....	65
<b>5.</b>	<b>Controls de seguretat física, de gestió i d'operacions .....</b>	<b>66</b>
5.1	CONTROLS DE SEGURETAT FÍSICA .....	66
5.1.1	Localització i construcció de les instal·lacions .....	66
5.1.2	Accés físic .....	67
5.1.3	Electricitat i aire condicionat .....	67
5.1.4	Exposició a l'aigua.....	67
5.1.5	Advertiment i protecció d'incendis .....	67
5.1.6	Emmagatzematge de suports.....	68
5.1.7	Tractament de residus.....	68
5.1.8	Còpia de seguretat fora de les instal·lacions .....	68

5.2	CONTROLS DE PROCEDIMENTS .....	68
5.2.1	Funcions fiables .....	69
5.2.2	Nombre de persones per tasca .....	69
5.2.3	Identificació i autenticació per a cada funció.....	69
5.2.4	Rols que requereixen separació de tasques.....	69
5.3	CONTROLS DE PERSONAL .....	70
5.3.1	Requisits d'historial, qualificacions, experiència i autorització.....	70
5.3.2	Requisits de formació .....	70
5.3.3	Requisits i freqüència d'actualització formativa.....	71
5.3.4	Seqüència i freqüència de rotació laboral.....	71
5.3.5	Sancions per accions no autoritzades .....	71
5.3.6	Requisits de contractació de professionals.....	71
5.3.7	Subministrament de documentació al personal .....	71
5.4	PROCEDIMENTS D'AUDITORIA DE SEGURETAT .....	71
5.4.1	Tipus d'esdeveniments registrats .....	71
5.4.2	Freqüència de tractament de registres d'auditoria .....	72
5.4.3	Període de conservació de registres d'auditoria .....	73
5.4.4	Protecció dels registres d'auditoria .....	73
5.4.5	Procediments de còpies de seguretat.....	73
5.4.6	Localització del sistema d'acumulació de registres d'auditoria.....	73
5.4.7	Notificació de l'esdeveniment d'auditoria al causant de l'esdeveniment.....	73
5.4.8	Anàlisi de vulnerabilitats .....	73
5.5	ARXIU D'INFORMACIONS .....	74
5.5.1	Tipus d'esdeveniments registrats .....	74
5.5.2	Període de conservació de registres .....	74
5.5.3	Protecció de l'arxiu .....	75
5.5.4	Procediments de còpia de suport .....	75
5.5.5	Requisits de segellat de cautela de data i hora .....	75
5.5.6	Localització del sistema d'arxiu .....	75
5.5.7	Procediments d'obtenció i verificació d'informació d'arxiu .....	76
5.6	RENOVACIÓ DE CLAUS .....	76
5.7	COMPROMÍS DE CLAUS I RECUPERACIÓ DE DESASTRE .....	76
5.7.1	Procediment de gestió d'incidències i compromisos .....	76
5.7.2	Corrupció de recursos, aplicacions o dades .....	76
5.7.3	Compromís de la clau privada de l'Entitat.....	76

5.7.4	Desastre sobre les instal·lacions .....	77
5.8	FINALITZACIÓ DEL SERVEI .....	77
5.8.1	Entitat de Certificació.....	77
5.8.2	Entitat de Registre.....	78
<b>6.</b>	<b>Controls de seguretat tècnica .....</b>	<b>79</b>
6.1	GENERACIÓ I INSTAL·LACIÓ DEL PARELL DE CLAUS .....	79
6.1.1	Generació del parell de claus .....	79
6.1.2	Tramesa de la clau privada al subscriptor .....	79
6.1.3	Tramesa de la clau pública a l'emissor del certificat .....	79
6.1.4	Distribució de la clau pública del Prestador de Serveis de Certificació .....	80
6.1.5	Mides de les claus.....	80
6.1.6	Generació de paràmetres de clau pública .....	80
6.1.7	Comprovació de qualitat de paràmetres de clau pública.....	80
6.1.8	Generació de les claus en aplicacions informàtiques o en béns d'equip.....	80
6.1.9	Propòsits d'ús de les claus .....	81
6.2	PROTECCIÓ DE LA CLAU PRIVADA.....	81
6.2.1	Mòduls de protecció de la clau privada.....	81
6.2.2	Control per més d'una persona (n de m) sobre la clau privada.....	82
6.2.3	Dipòsit de la clau privada .....	82
6.2.4	Còpia de seguretat de la clau privada .....	82
6.2.5	Arxiu de la clau privada .....	82
6.2.6	Introducció de la clau privada en el mòdul criptogràfic.....	83
6.2.7	Emmagatzematge de la clau privada en el mòdul criptogràfic .....	83
6.2.8	Mètode d'activació de la clau privada .....	83
6.2.9	Mètode de desactivació de la clau privada .....	83
6.2.10	Mètode de destrucció de la clau privada .....	83
6.2.11	Classificació dels mòduls criptogràfics .....	84
6.3	ALTRES ASPECTES DE GESTIÓ DEL PARELL DE CLAUS.....	84
6.3.1	Arxiu de la clau pública.....	84
6.3.2	Períodes d'utilització de les claus pública i privada.....	84
6.4	DADES D'ACTIVACIÓ.....	84
6.4.1	Generació i instal·lació de les dades d'activació .....	84
6.4.2	Protecció de dades d'activació .....	84
6.4.3	Altres aspectes de les dades d'activació .....	85
6.5	CONTROLS DE SEGURETAT INFORMÀTICA.....	85

6.5.1	Requisits tècnics específics de seguretat informàtica .....	85
6.5.2	Avaluació del nivell de seguretat informàtica .....	86
6.6	CONTROLS TÈCNICS DEL CICLE DE VIDA .....	86
6.6.1	Controls de desenvolupament de sistemes .....	86
6.6.2	Controls de gestió de seguretat .....	86
6.6.3	Avaluació del nivell de seguretat del cicle de vida .....	86
6.7	CONTROLS DE SEGURETAT DE XARXA.....	86
6.8	SEGELL DE TEMPS.....	87
<b>7.</b>	<b>Perfils de certificats i llistes de certificats revocats .....</b>	<b>88</b>
7.1	PERFIL DE CERTIFICAT.....	88
7.1.1	Número de versió .....	89
7.1.2	Extensions de certificat.....	89
7.1.3	Identificadors d'objecte d'algoritmes .....	89
7.1.4	Formats de noms .....	89
7.1.5	Restriccions de noms .....	90
7.1.6	Identificador d'objecte de política de certificat.....	90
7.1.7	Ús de l'extensió restriccions de política .....	90
7.1.8	Sintaxi i semàntica dels qualificadors de política .....	90
7.1.9	Semàntica del procés de l'extensió crítica de política de certificat .....	90
7.1.10	Especificacions tècniques per a totes les Entitats de Certificació .....	90
7.2	PERFIL DE LA LLISTA DE REVOCACIÓ DE CERTIFICATS.....	91
7.2.1	Número de versió .....	91
7.2.2	Llista de revocació de certificats i extensions d'elements de la llista.....	91
<b>8.</b>	<b>Auditoria de conformitat.....</b>	<b>92</b>
8.1	FREQÜÈNCIA DE L'AUDITORIA DE CONFORMITAT .....	92
8.2	IDENTIFICACIÓ I QUALIFICACIÓ DE L'AUDITOR .....	92
8.3	RELACIÓ DE L'AUDITOR AMB L'ENTITAT AUDITADA .....	92
8.4	RELACIÓ D'ELEMENTS OBJECTE D'AUDITORIA.....	93
8.5	ACCIONS A EMPRENDRE COM A RESULTAT D'UNA FALTA DE CONFORMITAT.....	93
8.6	TRACTAMENT DELS INFORMES D'AUDITORIA .....	93
<b>9.</b>	<b>Requisits comercials i legals.....</b>	<b>94</b>
9.1	TARIFES .....	94
9.1.1	Tarifa d'emissió o renovació de certificats .....	94
9.1.2	Tarifa d'accés a certificats .....	94
9.1.3	Tarifa d'accés a informació d'estat de certificat.....	94
9.1.4	Tarifes d'altres serveis.....	94
9.1.5	Política de reintegració .....	94



9.2	CAPACITAT FINANCERA.....	94
9.2.1	Assegurança de responsabilitat civil.....	94
9.2.2	Altres actius.....	95
9.2.3	Cobertura d'assegurança per a subscriptors i tercers que confiïn en certificats	95
9.3	CONFIDENCIALITAT.....	95
9.3.1	Informacions confidencials .....	95
9.3.2	Informacions no confidencials .....	95
9.3.3	Responsabilitat per a la protecció d'informació confidencial .....	95
9.4	PROTECCIÓ DE DADES PERSONALS .....	96
9.4.1	Política de Protecció de Dades Personals .....	96
9.4.2	Dades de caràcter personal no disponibles a tercers .....	97
9.4.3	Dades de caràcter personal disponibles a tercers .....	98
9.4.4	Responsabilitat corresponent a la protecció de les dades personals .....	98
9.4.5	Gestió d'incidències relacionades amb les dades de caràcter personal .....	99
9.4.6	Prestació del consentiment per al tractament de les dades personals.....	100
9.4.7	Comunicació de dades personals.....	100
9.5	DRETS DE PROPIETAT INTEL·LECTUAL .....	100
9.5.1	Propietat dels certificats i informació de revocació .....	100
9.5.2	Propietat de la política de certificació i la Declaració de Pràctiques de Certificació.....	101
9.5.3	Propietat de la informació relativa a noms.....	101
9.5.4	Propietat de claus.....	101
9.6	OBLIGACIONS I RESPONSABILITAT CIVIL.....	101
9.6.1	Entitats de Certificació.....	101
9.6.2	Entitats de Registre .....	106
9.6.3	Subscriptors .....	108
9.6.4	Verificadors .....	110
9.6.5	Altres Participants .....	111
9.7	RENÚNCIES DE GARANTIES.....	112
9.7.1	Rebuig de garanties de l'Entitat de Certificació.....	112
9.8	LIMITACIONS DE RESPONSABILITAT .....	112
9.8.1	Limitacions de responsabilitat de l'Entitat de Certificació vinculada .....	112
9.8.2	Cas fortuït i força major .....	112
9.9	INDEMNITZACIONS .....	112
9.9.1	Clàusula d'indemnitat de subscriptor .....	112

9.9.2	Clàusula d'indemnitat de verificador .....	112
9.10	TERMINI I ACABAMENT .....	113
9.10.1	Termini .....	113
9.10.2	Acabament .....	113
9.10.3	Supervivència .....	113
9.11	NOTIFICACIONS .....	113
9.12	MODIFICACIONS .....	114
9.12.1	Procediment per a les modificacions .....	114
9.12.2	Període i mecanismes per a notificacions .....	114
9.12.3	Circumstàncies en què un OID ha de ser canviat .....	114
9.13	RESOLUCIÓ DE CONFLICTES .....	114
9.13.1	Resolució extrajudicial de conflictes .....	114
9.13.2	Jurisdicció competent .....	115
9.14	LLEI APLICABLE .....	115
9.15	CONFORMITAT AMB LA LLEI APLICABLE .....	115
9.16	CLÀUSULES DIVERSES .....	115
9.16.1	Acord íntegre .....	115
9.16.2	Subrogació .....	116
9.16.3	Divisibilitat .....	116
9.16.4	Aplicacions .....	116
9.16.5	Altres clàusules .....	116
<b>ANNEX I</b>	<b>.....</b>	<b>117</b>
	CONTROL DOCUMENTAL .....	117
	CONTROL DE VERSIONS PGdC 2N SEMESTRE 2011 .....	117

## 1. Introducció

En desenvolupament del 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 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 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 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 de 2002 va tenir lloc la sessió constitutiva del Consorci per a l'Administració Oberta Electrònica de Catalunya, una sessió en què el Consell General va adoptar, 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), 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 de 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 de 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 les institucions de règim 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, anomenada "jerarquia pública de certificació de Catalunya", i podran admetre i utilitzar certificats d'altres prestadors mitjançant els serveis de classificació i validació de CATCert.

Un dels elements més importants de la jerarquia pública de certificació de Catalunya és la redacció i la publicació d'una política general de certificació - continguda en aquest document - que, en forma de requisits i condicions, serà aplicable a tots els certificats que s'emeten a persones físiques i jurídiques per les diferents entitats de certificació que es vinculin a la jerarquia. Així mateix, els requisits i condicions establerts en aquesta política han d'ajudar a l'homologació de les polítiques de certificats de tercers prestadors, a efectes de l'oportuna classificació i admissió per les administracions públiques catalanes dels esmentats certificats.

L'aparició de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, implica el reconeixement de les especificitats de la signatura electrònica de les administracions públiques, amb la regulació dels certificats digitals corresponents a la seu electrònica, el segell d'actuació administrativa automatitzada i la signatura electrònica del personal al servei de les administracions públiques, refermant l'aproximació inicialment adoptada per CATCert per a la prestació dels seus serveis. Tanmateix, la regulació proposada exigeix la revisió dels continguts de la política general de certificació en relació amb els nous tipus de certificats, sense afectar a la resta del model de certificació del sistema públic català.

CATCert compleix amb la versió actual de les pautes del CA/Browser Fòrum per a l'emissió i gestió de certificats de validació extesa ("extended validation") publicades a <http://www.cabforum.org>.

## 1.1 Presentació

### 1.1.1 Tipus i classes de certificats

L'Agència Catalana de Certificació ha definit una tipologia de serveis de certificació, a fi d'expedir certificats digitals per a diversos usos i diferents usuaris finals, i per poder classificar altres certificats emesos per prestadors de serveis de certificació, classificació que es basa, a més d'en altres criteris oportunament publicats, en la comparació d'aquests certificats d'altres prestadors amb els que emet l'Agència Catalana de Certificació.

Per aquest motiu, resulta important que tots els usuaris coneguin en detall el contingut d'aquest document, ja que han de decidir quins certificats necessiten sol·licitar a CATCert, així com quan han d'emprar certificats de tercers prestadors.

En primer lloc, dins de la jerarquia pública de certificació de Catalunya, operada per CATCert, s'expedeixen certificats a altres Entitats de Certificació, que d'aquesta forma queden vinculades a la jerarquia. Aquests certificats s'anomenen Certificats d'Infraestructura d'Entitat de Certificació (CIC), i permeten que les entitats de certificació subscriptores dels certificats CIC puguin expedir certificats a altres Entitats de Certificació o a usuaris finals.

Els CIC s'expedeixen per oferir serveis a una comunitat d'usuaris concreta (per exemple, el personal de la Generalitat de Catalunya, o de les entitats que integren l'Administració local, o els ciutadans, o els docents i estudiants universitaris, entre altres exemples) dins de la jerarquia pública de certificació de Catalunya, podent ser de diferents nivells (1, 2 o successius).

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

Cada certificat CIC rebrà un nivell, adequat al període de durada del mateix, que s'emprarà per a la programació de la renovació periòdica de la infraestructura de certificació.

Els certificats d'usuaris finals es divideixen en:

- Certificats personals, caracteritzats pel fet que el posseïdor de la clau privada és una persona física, que actua en el seu propi nom i representació (sent en aquest

cas subscriptor o titular del certificat), o en representació i per compte d'una persona jurídica (que serà el subscriptor o titular del certificat)

- Certificats d'entitat, caracteritzats pel fet, que el subscriptor del certificat i, d'acord amb la llei, signant, és una persona jurídica, que actua per mitjà d'un posseïdor de claus (també anomenat per a aquests certificats com "responsable de custòdia")
- Certificats de dispositiu, caracteritzats pel fet que el posseïdor de la clau privada és un dispositiu informàtic que realitza les operacions de signatura i desxifrat de forma automàtica, sota la responsabilitat d'una persona física o jurídica (anomenat subscriptor o titular del certificat), i
- Certificats d'objecte, caracteritzats pel fet que el posseïdor de la clau privada podrà accedir i gestionar un objecte, com un sobre digital, que requereix serveis criptogràfics per a la gestió citada.

Els certificats d'usuari final (personals i d'entitat) s'emeten en dues modalitats:

- Els certificats de Classe 1 són certificats públics, d'organització del sector públic (corporatius), caracteritzats pel fet que la persona física posseïdora de la clau privada té una vinculació amb el subscriptor o titular del certificat, que és una persona jurídica. A més, en certificats d'entitat, el posseïdor de la clau privada ha estat facultat, d'acord amb la llei d'atribucions aplicable, per a l'obtenció del certificat. La persona física posseïdora de la clau privada estarà identificada al certificat. Es preveu la possibilitat d'utilitzar pseudònims en casos especials com poden ser certificats de cossos de seguretat o de personal vinculat a l'administració de justícia.

Habitualment el subscriptor actua com a entitat de registre dels certificats, encara que no és estrictament necessari, ja que pot acordar que aquesta funció la practiqui CATCert o una Entitat de Registre Col·laboradora autoritzada per CATCert.

- La resta de certificats seran certificats de classe 2, emesos en concurrència amb el lliure mercat, i habitualment en règim d'actuació subsidiària, quan no existeixin prestadors que ofereixin el servei o el nombre dels mateixos resulti insuficient per garantir la seva distribució efectiva als usuaris finals (ciutadans, empreses, professionals). El registre de les dades per a l'emissió dels certificats de classe 2 el realitza sempre l'Entitat de Certificació o una entitat de registre sota la responsabilitat de l'Entitat de Certificació, que mai pot ser un subscriptor individual dels certificats.

Els certificats de classe 2 poden ser individuals o d'organització del sector privat o del sector públic fora de Catalunya (corporatius), depenent de si s'expedeixen a una persona física, actuant en el seu propi nom, o a una organització, que actua per mitjà d'una persona física, identificada al certificat - encara que sigui mitjançant un pseudònim.

D'aquesta manera, les Entitats de Certificació de la jerarquia pública de certificació de Catalunya podran, en funció de les seves necessitats i de la situació conjuntural del mercat de serveis de certificació, emetre els següents grups de certificats:

- Certificats d'entitat de certificació de nivell 2 o superior.
- Certificats personals de classe 1 i de classe 2.

- Certificats d'entitat de classe 1 i de classe 2.
- Certificats de dispositius de classe 1 i de classe 2.
- Certificats d'objecte de classe 1 i de classe 2.

Per la seva part, resulta competència exclusiva de CATCert emetre els certificats d'entitat de certificació de nivell 1 a noves Entitats de Certificació.

A continuació es detallen les diferents polítiques de certificats d'infraestructura, personals, d'entitat, de dispositiu i d'objecte, tant de classe 1 com de classe 2, que s'ofereixen a les Entitats de Certificació i a la comunitat d'usuaris, així com les possibles combinacions i ampliacions per a usos concrets de les mateixes.

#### 1.1.1.1 Certificats d'infraestructura

Podran existir set 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 què hagin obtingut un certificat CIC vàlid, i mentre l'esmentat certificat es trobi vigent.

- 2) Certificat d'infraestructura personal de signatura electrònica reconeguda d'operadors (CIPISR), que s'utilitza 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 és utilitzat per a una aplicació informàtica servidor de SSL o de TLS d'infraestructura per identificar-se davant de 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 és utilitzat per aplicacions informàtiques de la infraestructura que s'identifiquen digitalment, signin 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 és utilitzat per 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 és utilitzat per una entitat per signar els segells de temps que emet.
- 7) Certificat d'infraestructura d'entitat de validació (CIV), que és utilitzat per un servidor d'entitat de validació per signar els seus informes.



### 1.1.1.2 Certificats personals

Podran existir quatre tipus de certificats personals:

- 1) Certificats personals de signatura electrònica reconeguda (CPSR), d'acord amb l'establert a l'article 6 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, que permeten que persones físiques, a títol individual o per raó de la seva vinculació amb una institució jurídic-pública o privada (càrrec, atribució, apoderament) signin documents amb dispositiu segur de creació de signatura.
- 2) Certificats personals de signatura electrònica avançada (CPSA), d'acord amb l'establert a l'article 6 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, que permeten que persones físiques, a títol individual o per raó de la seva vinculació amb una institució jurídic-pública o privada (càrrec, atribució, apoderament) signin documents sense dispositiu segur de creació de signatura.
- 3) Certificats personals d'identitat (CPI), que s'utilitzen per signar missatges d'autenticació (confirmació de la identitat) i d'accés segur a sistemes informàtics.
- 4) Certificats personals de xifrat (CPX), que s'utilitzen per produir o rebre documents o missatges confidencials.

Les anteriors polítiques permeten combinacions entre elles, depenent de les necessitats dels usuaris, de manera que un únic certificat pot donar compliment a més d'una política. Per exemple, resulta freqüent combinar les polítiques de signatura reconeguda i d'identificació en un únic certificat.

Addicionalment, en funció dels requisits tècnics i les necessitats dels usuaris, és possible que els esmentats tipus de certificat puguin incorporar altres funcionalitats que, en tot cas, seran identificades en cada Declaració de Pràctiques de Certificació que adopti aquests tipus.

Es podrà crear un tipus específic del certificat CPSR, CPSA, CPI i CPX adreçat, al menys, al personal al servei de les administracions públiques catalanes, d'acord amb l'article 19 de la Llei 11/2007, de 22 de juny.

### 1.1.1.3 Certificats d'entitat

Podran existir quatre tipus de certificats d'entitat:

- 1) Certificats d'entitat de signatura electrònica reconeguda (CESR), d'acord amb l'establert a l'article 7 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, que permeten que institucions públiques i privades, corporacions de dret públic i persones jurídic-públiques (col·lectivament anomenades "entitats") signin documents amb dispositiu segur de creació de signatura.
- 2) Certificats d'entitat de signatura electrònica avançada (CESA), segons la definició del punt 2 de l'article 3 de la Llei 59/2003, de 19 de desembre, de signatura electrònica i d'acord amb l'establert a l'article 7 de la mateixa llei.
- 3) Certificats d'entitat per a identificació (CEI) que s'utilitzen per signar missatges d'autenticació (confirmació de la identitat) i d'accés segur a sistemes informàtics.
- 4) Certificats d'entitat de xifrat (CEX), d'acord amb l'establert a l'article 7 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, que permeten que

institucions públiques i privades, corporacions de dret públic i persones jurídico-públiques (col·lectivament anomenades "entitats") puguin produir i rebre documents confidencials.

Adicionalment, en funció dels requisits tècnics i les necessitats dels usuaris, és possible que els esmentats tipus de certificat puguin incorporar altres funcionalitats que, en tot cas, seran identificades en cada Declaració de Pràctiques de Certificació que adopti aquests tipus.

#### 1.1.1.4 Certificats de dispositiu

Podran existir quatre tipus de certificat de dispositiu:

- 1) Certificat de signatura d'aplicacions informàtiques (CDP), que s'utilitza per signar digitalment aplicacions informàtiques a transmetre per mitjà de xarxes.
- 2) Certificat de dispositiu servidor segur (CDS), que és ocupat per una aplicació informàtica servidor de SSL o de TLS per a identificar-se davant de les aplicacions client que es connectin i per protegir el secret de les comunicacions entre el client i el servidor.
- 3) Certificat de dispositiu d'aplicació digitalment assegurada (CDA), que és utilitzat per aplicacions informàtiques que s'identifiquen digitalment, signen electrònicament *webservices* o altres protocols i que generen i reben documents i missatges xifrats.
- 4) Certificat de dispositiu de xifrat (CDX), que s'utilitza per al xifrat automàtic de les comunicacions entre els dispositius identificats als certificats, per establir xarxes privades virtuals.

Adicionalment, en funció dels requisits tècnics i les necessitats dels usuaris, és possible que els esmentats tipus de certificat puguin incorporar altres funcionalitats que, en tot cas, seran identificades en cada Declaració de Pràctiques de Certificació que adopti aquests tipus.

Es podran crear tipus específics dels certificats CDS, i CDA adreçats, almenys, a la seu electrònica i a les aplicacions d'actuació administrativa automatitzada de les administracions públiques catalanes, d'acord amb l'article 19 de la Llei 11/2007, de 22 de juny.

#### 1.1.1.5 Certificats d'objecte

Podrà existir un tipus de certificat d'objecte:

- 1) Certificat d'objecte sobre digital administratiu (COS), que s'utilitza per xifrar documentació dins d'un sobre digital que només es podrà obrir quan arribi la data indicada en el mateix sobre.

Adicionalment, en funció dels requisits tècnics i les necessitats dels usuaris, és possible que els esmentats tipus de certificat puguin incorporar altres funcionalitats que, en tot cas, seran identificades en cada Declaració de Pràctiques de Certificació que adopti aquest tipus.



### 1.1.1.6 Certificats de proves

De qualsevol dels tipus de certificats que recull la present política es poden emetre, sota determinades circumstàncies, certificats de prova.

## 1.1.2 Relació entre la política de certificació i altres documents

Aquest document conté la política general de certificació de l'Agència Catalana de Certificació. Una política de certificació és un conjunt de principis i regles relatius a l'emissió i gestió de certificats digitals, amb suport de claus públiques, que poden utilitzar-se en diferents serveis, com l'autenticació de la identitat, la integritat i l'autenticitat<sup>1</sup> documental o el secret de les dades, documents i transmissions.

La política de certificació estableix les regles mínimes que s'han de complir per part de les Entitats de Certificació, els subscriptors i altres usuaris de certificats.

D'altra banda, cada Entitat de Certificació ha de disposar d'una Declaració de Pràctiques de Certificació amb els procediments que aplica en la prestació dels seus serveis, en compliment de l'establert a l'article 19 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, indicant el grau d'aplicació dels requisits establerts per les polítiques de certificats que gestiona i detallant les seves pràctiques professionals en relació amb la provisió dels serveis de certificació.

Aquesta documentació es relaciona amb la documentació auxiliar, entre la que es troben els instruments jurídics reguladors de la prestació del servei (documentació jurídica auxiliar), documentació de seguretat, documentació d'operacions i d'arxiu.

## 1.1.3 Termes habituals utilitzats en aquest document

A continuació, per facilitar la comprensió del document, s'aporten breus definicions dels termes més utilitzats en aquest document:

Certificat	Document electrònic signat per una entitat de certificació, que vincula unes dades de verificació de signatura electrònica a una entitat (persona física o jurídica) i confirma la seva identitat
Declaració de pràctiques de certificació	Document exigít per la Llei de signatura electrònica, que detalla els requisits que compleix el prestador de serveis de certificació quan emet certificats.
Entitat de certificació	Persona física o jurídica que emet certificats, d'acord amb la Llei de signatura electrònica. De vegades, es tracta com un

<sup>1</sup> Concepte que correspon a l'anomenat "no repudi" (en anglès, "non-repudiation").

	sinònim d'autoritat de certificació, que és un component tècnic del servei.
Entitat de certificació arrel	Entitat de certificació superior de la jerarquia de certificació, que garanteix legalment tots els certificats emesos per les entitats de certificació vinculades a la jerarquia.
Entitat de certificació vinculada	Entitat de certificació que ha estat vinculada a una jerarquia de certificació, de manera que l'entitat de certificació superior garanteix els certificats emesos per l'entitat vinculada.
Entitat de certificació virtual	Entitat de certificació que ha delegat totes les operacions tècniques per a l'emissió dels certificats a un prestador de serveis de certificació.
Entitat de registre	Persona física o jurídica que executa els procediments de comprovació de la identitat i de la resta de circumstàncies dels subscriptors i posseïdors dels certificats. De vegades es tracta com un sinònim d'autoritat de registre, que és un component tècnic del servei.
Entitat de registre col·laboradora	Entitat de registre que col·labora amb les entitats de certificació en l'emissió dels certificats als subscriptors.
Entitat de registre interna	Entitat de registre d'una administració subscriptora de certificats, que registra els seus posseïdors de claus.
Entitat de registre virtual	Entitat de registre interna que ha delegat en l'entitat de certificació o en una entitat de registre col·laboradora els treballs tècnics del procediment de comprovació de la identitat i de la resta de circumstàncies personals dels subscriptors i dels posseïdors dels certificats.
Jerarquia pública de certificació de Catalunya	Conjunt d'entitats públiques i catalanes de certificació, entitats de registre i altres que emeten certificats, organitzades en un sistema públic controlat i garantit per l'Agència Catalana de Certificació, que actua com a entitat de certificació arrel per delegació de les institucions de règim d'autogovern de Catalunya, i de les administracions públiques catalanes.

Llista de revocació de certificats

Document electrònic signat per una entitat de certificació que detalla els certificats que, temporalment o definitivament, no són vàlids.

Perfil de certificat

Document que detalla els continguts dels certificats, sintàcticament i semànticament.

Posseïdor de claus

Persona física que rep un certificat emès a un subscriptor col·lectiu, i que l'utilitza sota la responsabilitat del subscriptor.

Prestador de serveis de certificació

Persona física o jurídica que actua legalment com a entitat de certificació o que presta serveis de certificació a tercers, per delegació d'una entitat de certificació.

Segell electrònic

D'acord amb la Llei 11/2007, de 22 de juny, d'Accés Electrònic dels Ciutadans als Serveis Públics, es tracta d'un sistema de signatura electrònica per a l'actuació administrativa automatitzada, basat en certificat electrònic.

Seu electrònica

D'acord amb la Llei 11/2007, de 22 de juny, d'Accés Electrònic dels Ciutadans als Serveis Públics, és l'adreça electrònica disponible per als ciutadans a través de xarxes de telecomunicacions la titularitat, gestió i administració de la qual correspon a una Administració Pública, òrgan o entitat administrativa en l'exercici de les seves competències.

Sistema públic català de certificació

Conjunt de totes les entitats, públiques i privades, catalanes, nacionals i internacionals, de certificació, entitats de registre i altres que emetin certificats, organitzades en un sistema públic controlat i garantit per l'Agència Catalana de Certificació, que actua com a entitat de classificació per delegació de les institucions d'autogovern de Catalunya, i de les administracions públiques catalanes.

Subscriptor

Persona física o jurídica que contracta el servei de certificació, per a ús individual o col·lectiu.

## 1.2 Nom del document i identificació

Aquest document de polítiques de certificació de la jerarquia s'anomena "Política general de certificació – Agència catalana de Certificació".

Aquest document no rep un OID, donat el seu caràcter general. Al contrari, cada tipus de certificat (d'acord amb una política bàsica, resultant d'una combinació de polítiques o d'una política específica de certificat d'aplicació general) rep el seu propi OID, que s'identifica a cada Declaració de Pràctiques de Certificació de cada Entitat de Certificació que emet un tipus concret de certificat, i que s'ha d'incloure dins del certificat, en el camp "Informació de política" (Policy Information), excepte quan no resulti possible tècnicament.

Cada Entitat de Certificació Vinculada podrà, abans de començar a emetre certificats, establir la seva pròpia política de certificat, a partir de l'establert en aquest document per a cada tipus i classe de certificat, concretant o establint noves normes de certificació, amb absolut respecte a les normes d'aquesta política.

Les polítiques específiques poden ser de dos tipus:

- a) Polítiques que defineixen normes aplicables a tota la comunitat d'usuaris, amb independència de l'Entitat de Certificació que emeti el certificat, per exemple la creació d'un tipus específic de certificat CPSR, incloent el càrrec, política que pot ser aplicable a altres Entitats de Certificació.
- b) Polítiques que defineixin o adaptin normes aplicables a una part de la comunitat d'usuaris, generalment dependent d'una Entitat de Certificació concreta, per exemple l'adaptació d'un CPSR a les necessitats concretes d'una Entitat de Certificació, que pot no tenir sentit per a altres Entitats de Certificació.

Per a determinades polítiques s'introdueix el concepte de "nivell", en referència a la robustesa criptogràfica de les claus, a la seva generació i a la seva custòdia i aplicació. Podran existir dos nivells en relació amb el tipus de certificat:

- a) Nivell alt: La generació, custòdia i aplicació de la clau privada ha de realitzar-se:
  - a. per als certificats personals i d'entitat, en dispositiu segur de creació de signatura, d'acord amb la llei 59/2003
  - b. per als certificats de dispositiu, en maquinari criptogràfic que compleixi els requisits establerts a qualsevol perfil de protecció o *security target*, escrit d'acord amb CC EAL 3 o FIPS 140-1 o -2 nivell 2, que incorpori els requisits del CEN *Workshop Agreement* CWA14167-1 per a certificats no qualificats (reconeguts) o de conformitat amb qualsevol perfil de protecció o *security target*, escrit d'acord amb altres esquemes de certificació (ITSEC), que incorpori els requisits de CEN *Workshop Agreement* CWA14167-1 per a certificats no qualificats (reconeguts).
- b) Nivell mig: la generació, custòdia i aplicació de la clau privada pot realitzar-se en mòduls criptogràfics en programari i els algorismes i els seus paràmetres seran els comunament utilitzats.

Cada política bàsica de certificat, cada combinació de polítiques de certificat, i cada política específica de certificat disposarà del seu propi OID, que s'especificarà a la Declaració de Pràctiques de Certificació corresponent.

Aquest OID serà assignat per l'Agència Catalana de Certificació, dins de la seva branca d'OIDs 1.3.6.1.4.1.15096.1.3.1. D'aquesta manera es demostrarà la conformitat del tipus de certificat amb aquesta política general<sup>2</sup>.

## 1.3 Comunitat d'usuaris de certificats

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

Els certificats de classe 1 expedits per les Entitats de Certificació Vinculades no s'expedeixen al públic, sinó 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 i els reben i utilitzen el seu personal, els seus dispositius i els objectes que gestionen.

En canvi, els certificats de classe 2 es poden expedir al públic o en entorns tancats d'usuaris, en especial en relacions administratives de subjecció, en lliure concurrència amb altres prestadors de serveis de certificació.

### 1.3.1 Prestadors de serveis de certificació

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

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

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

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

#### 1.3.1.1 Prestadors de serveis de certificació de les institucions

CATCert serà el principal prestador de serveis de certificació de les institucions i, en concret, oferirà serveis a diverses entitats de certificació de les institucions, que regeixen diferents comunitats d'usuaris, amb els corresponents sistemes tècnics d'autoritat de certificació diferenciats i vinculats a la jerarquia pública de certificació de Catalunya.

En la seva funció de prestador de serveis de certificació de les institucions, CATCert serà responsable, davant dels seus usuaris finals i, en especial, dels tercers verificadors de

---

<sup>2</sup> TS 101 456: 8.4; TS 102042: 8.3

certificats i signatures electròniques, per l'actuació dels sistemes tècnics d'autoritat de certificació que opera en nom de les diferents entitats de certificació.

En el cas que una entitat de certificació sigui operada directament per una institució, constituïda com a prestador de serveis de certificació, amb el seu propi sistema tècnic d'autoritat de certificació, aquesta entitat de certificació podrà integrar-se en el sistema públic català de certificació mitjançant la vinculació tècnica de l'esmentat sistema d'autoritat de certificació en la jerarquia pública de certificació de Catalunya.

### 1.3.1.2 Prestadors de serveis de certificació classificats

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

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

### 1.3.2 Entitat de Certificació Arrel

L'Entitat de Certificació Arrel és CATCert, que disposa d'un sistema tècnic d'autoritat de certificació principal, que té la finalitat que s'integrin altres entitats de certificació al sistema públic català de certificació mitjançant la vinculació tècnica de les autoritats de certificació corresponents a la jerarquia pública de certificació de Catalunya.

Aquesta vinculació tècnica s'aconsegueix mitjançant l'emissió dels certificats CIC, de nivell 1 i de nivell 2.

### 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 gestió dels certificats mitjançant les autoritats de certificació, i que es troben inscrites en 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 roman responsable de l'organització i les decisions de gestió referides a l'entitat de certificació. Aquesta funció, que no pot ser objecte de delegació, es diu Entitat de Certificació Virtual.

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

### 1.3.4 Entitats de Registre

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

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

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

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

Existeixen tres tipus d'Entitats de Registre:

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

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

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

### 1.3.5 Usuaris finals

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

- a) Els sol·licitants de certificats.
- b) Els subscriptors de certificats.



- c) Els posseïdors de claus.
- d) Els verificadors de signatures, segells i certificats.

### 1.3.5.1 Sol·licitants de certificats

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

Poden ser sol·licitants:

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

L'autorització del sol·licitant podrà realitzar-se tant de forma expressa com tàcita, i en aquells casos en els quals l'entitat de certificació el consideri convenient podrà formalitzar-se documentalment

### 1.3.5.2 Subscriptors de certificats

Els subscriptors són les institucions i les persones, físiques o jurídiques, així identificades en el camp "Subject" del certificat.

En certificats de dispositiu, en el camp "Subject" també s'identifica el dispositiu, i en certificats d'objecte, en el camp "Subject" també s'identifica l'objecte.

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

### 1.3.5.3 Posseïdors de claus

Els posseïdors de claus són les persones físiques que posseeixen de forma exclusiva les claus de signatura digital de certificats personals o d'entitat, de classe 1 o de classe 2 d'organització, que es troben degudament autoritzats per a això pel subscriptor i que han estat degudament identificades al certificat mitjançant el seu nom i cognoms o mitjançant un pseudònim.

Als certificats d'entitat, a més, els posseïdors de claus han de tenir en compte l'establert a l'article 7 de la Llei 59/2003, de 19 de desembre, quant a la custòdia de les claus del certificat.

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



### 1.3.5.4 Verificadors de certificats

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

## 1.4 Ús dels certificats

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

### 1.4.1 Usos típics del certificats

#### 1.4.1.1 Requisits específics per al CIC

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

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

Els CIC s'obtenen després d'un procés d'admissió de l'Entitat de Certificació Vinculada als serveis de certificació de l'Agència Catalana de Certificació.

#### 1.4.1.2 Requisits específics per al CPIISR

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

#### 1.4.1.3 Requisits específics per al CIDS

Els certificats d'infraestructura de dispositiu servidor segur (CIDS) s'emeten a Entitats de Certificació, responsables de l'operació de servidors segurs SSL o TLS, amb els següents usos:

- d) Autenticació de servidor.
- e) Xifrat de les comunicacions entre client i servidor.

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

#### 1.4.1.4 Requisits específics per al CIDA

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

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

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

#### 1.4.1.5 Requisits específics per al CIO

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

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

#### 1.4.1.6 Requisits específics per al CIT

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

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

#### 1.4.1.7 Requisits específics per al CIV

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

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

#### 1.4.1.8 Requisits específics per al CPSR

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

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

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

Els certificats CPSR poden incloure una manifestació relativa a la categoria de personal i càrrec del posseïdor de claus, que han estat comprovats abans d'emetre el certificat.

#### 1.4.1.9 Requisits específics per al CPSA

Els certificats personals de signatura avançada (d'ara endavant, CPSA) són certificats reconeguts d'acord amb el que s'estableix a l'article 11.1, amb el contingut prescrit per l'article 11.1, amb el contingut prescrit per l'article 11.2, i emesos complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que donen compliment a allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Els CPSA no funcionen necessàriament amb dispositiu segur de creació de signatura electrònica d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre.

Els CPSA garanteixen la identitat del subscriptor i, en el seu cas, del posseïdor de la clau de signatura, resultant idonis per oferir suport a la signatura electrònica avançada.

Encara que la signatura electrònica avançada no s'equipara directament a la signatura escrita, aquesta equiparació es pot produir igualment en virtut d'un contracte de signatura electrònica o d'una norma jurídica específica, que establirà les condicions addicionals necessàries perquè es produeixi l'esmentada equiparació.

#### 1.4.1.10 Requisits específics per al CPI

Els certificats personals d'identitat (CPI) es poden utilitzar per a diversos usos, entre els quals es poden indicar els següents:

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

Els CPI són certificats reconeguts, i garanteixen la identitat del subscriptor i, en el seu cas, del posseïdor de la clau de signatura.

#### 1.4.1.11 Requisits específics per al CPX

Els certificats personals de xifrat (CPX) es poden utilitzar exclusivament per produir o rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge utilitzant la clau pública del subscriptor indicada en el CPX.

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

Els CPX garanteixen la identitat del subscriptor, però no permeten la signatura electrònica de missatges de dades.

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

#### 1.4.1.12 Requisits específics per al CESR

Els certificats d'entitat de signatura reconeguda (CESR) són certificats reconeguts, d'acord amb l'establert a l'article 11.1, amb el contingut prescrit per l'article 11.2, i emès seguint les prescripcions dels articles 7, 12, 13 i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que donen compliment al disposat en la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions identificada amb la referència TS 101 456.

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

Per aquest motiu, els CESR garanteixen la identitat del subscriptor i del responsable de la custòdia de la clau privada de signatura, resultant idonis per oferir suport a la signatura electrònica reconeguda de l'entitat; és a dir, la signatura electrònica avançada que es basa en certificat reconegut i que ha estat generada utilitzant un dispositiu segur, pel qual, d'acord amb l'article 3.4 de la Llei 59/2003, de 19 de desembre, s'equipara a la signatura manuscrita per efecte legal, sense necessitat de complir cap requisit addicional més.

#### 1.4.1.13 Requisits específics per al CESA

Els certificats d'entitat de signatura avançada (CESA) són certificats reconeguts, d'acord amb l'establert a l'article 11.1, amb el contingut prescrit per l'article 11.2, i emès seguint les prescripcions dels articles 7, 12, 13 i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que donen compliment al disposat en la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions identificada amb la referència TS 101 456.

Els CESA no funcionen necessàriament amb dispositiu segur de creació de signatura electrònica d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre.

Els CESA garanteixen la identitat del subscriptor i del responsable de la custòdia de la clau privada de signatura, resultant idonis per oferir suport a la signatura electrònica avançada.

Encara que la signatura electrònica avançada no s'equipara directament a la signatura escrita, aquesta equiparació es pot produir igualment en virtut d'un contracte de signatura electrònica o d'una norma jurídica específica, que establirà les condicions addicionals necessàries perquè es produeixi l'esmentada equiparació.

#### **1.4.1.14 Requisits específics per al CEI**

Els certificats d'entitat per a identificació (CEI) es poden utilitzar per a diversos usos, entre els quals es poden indicar els següents:

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

Els CEI són certificats reconeguts, i garanteixen la identitat del subscriptor i, en el seu cas, del posseïdor de la clau de signatura.

#### **1.4.1.15 Requisits específics per al CEX**

Els certificats d'entitat de xifrat (CEX) són certificats reconeguts, que s'expedeixen a subscriptors i es poden utilitzar exclusivament per xifrar o rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, utilitzant la clau pública del subscriptor indicada en el CEX.

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

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

#### **1.4.1.16 Requisits específics per al CDS**

Els certificats de dispositiu servidor segur (CDS) s'emeten a institucions responsables de l'operació de servidors segurs SSL o TLS, amb els següents usos:

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

Els certificats CDS són certificats ordinaris, que garanteixen la identitat del servidor concret on funcionen.

Els certificats CDS-1 Seu electrònica només es poden subministrar a les administracions públiques, òrgans o entitats administratives, d'acord amb l'article 10 de la Llei 11/2007, i han de complir els requisits de l'article 17 de la Llei 11/2007.

#### 1.4.1.17 Requisits específics per al CDP

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

Els certificats CDP són certificats ordinaris, que garanteixen la identitat de la institució editora i l'origen i la integritat del programari signat.

#### 1.4.1.18 Requisits específics per al CDA

Els certificats de dispositiu d'aplicació digitalment assegurada s'emeten a persones jurídiques responsables de l'operació d'aplicacions informàtiques que s'identifiquen digitalment, signen electrònicament *webservices* o altres protocols i que produeixen i reben documents i missatges xifrats.

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

Els certificats CDA-1 Segell electrònic només es poden subministrar a les administracions públiques, òrgans o entitats administratives, per a l'exercici de la competència administrativa de forma automatitzada, i han de complir els requisits de l'article 18 de la Llei 11/2007.

#### 1.4.1.19 Requisits específics per al COS

Els certificats d'objecte sobre digital administratiu s'emeten a òrgans de contractació per a la seva publicació i ús en les licitacions electròniques que els requereixin, com les previstes pel Decret 96/2004, de 20 de gener.

### 1.4.2 Aplicacions prohibides

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

Els certificats d'entitats finals no es poden utilitzar per signar peticions d'emissió, renovació, suspensió, habilitació o revocació de certificats, ni per signar certificats de clau pública de cap tipus, ni signar llistes de revocació de certificats (LRC).

Els certificats de signatura no es poden utilitzar per signar missatges d'autenticació incomprensibles per al signant, en particular desafiaments de client SSL o TLS, excepte quan es combinin amb un certificat d'identitat, i tampoc es poden utilitzar per rebre missatges xifrats, excepte quan es combinin amb un certificat de xifratge i no s'emmagatzemi la clau privada.

L'ús dels certificats amb indicació de càrrec queda restringit per a les tasques pròpies del càrrec i pels usos inclosos al certificat.

#### **1.4.2.1 Requisits específics per al CIC**

Els certificats CIC s'atindran al disposat en aquesta política i, en tot cas, les limitacions estaran delimitades per la classe del certificat CIC, així com s'especifica en l'esmentat punt i, en el seu cas, per la política de certificat concreta.

#### **1.4.2.2 Requisits específics per al CIPISR**

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

#### **1.4.2.3 Requisits específics per al CIDS**

Els CIDS no es poden utilitzar en sistemes diferents del de l'Entitat de Certificació.

#### **1.4.2.4 Requisits específics per al CIDA**

Els CIDA no es poden utilitzar en sistemes diferents dels de l'Entitat de Certificació.

#### **1.4.2.5 Requisits específics per al CIO**

Els CIO no es poden utilitzar en sistemes diferents dels de l'Entitat de Certificació.

#### **1.4.2.6 Requisits específics per al CIT**

Els CIT no es poden utilitzar en sistemes diferents dels de l'Entitat de Certificació.

#### **1.4.2.7 Requisits específics per al CIV**

Els CIV no es poden utilitzar en sistemes diferents dels de l'Entitat de Certificació.

#### **1.4.2.8 Requisits específics per al CPSR**

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

Els CPSR tampoc no poden utilitzar-se per signar missatges d'autenticació incomprensibles per al signant, en particular desafiaments de client SSL o TLS, excepte quan es combinin amb un CPI, i tampoc es poden utilitzar per rebre missatges xifrats, excepte quan es combinin amb un CPX i no s'emmagatzemi la clau privada.



#### **1.4.2.9 Requisits específics per al CPSA**

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

Els CPSA tampoc no poden utilitzar-se per signar missatges d'autenticació incomprensibles per al signant, en particular desafiaments de client SSL o TLS, excepte quan es combinin amb un CPI, i tampoc es poden utilitzar per rebre missatges xifrats, excepte quan es combinin amb un CPX i no s'emmagatzemi la clau privada.

#### **1.4.2.10 Requisits específics per al CPI**

Els CPI no poden utilitzar-se per signar peticions d'emissió, renovació, suspensió o revocació de certificats CIC, certificats de cap tipus, o llistes de revocació de certificats (LRC), i tampoc no es poden utilitzar per rebre missatges xifrats, excepte quan es combinin amb un CPX.

#### **1.4.2.11 Requisits específics per al CPX**

Els CPX no poden utilitzar-se per generar signatures digitals de cap tipus de missatge de dades, excepte quan es combinin amb un CPSR - si la clau privada no s'emmagatzema -, CPSA o CPI.

#### **1.4.2.12 Requisits especials per als certificats amb Càrrec i Càrrec amb Ús**

A més de les restriccions pròpies de les polítiques bàsiques en les que es basen aquest certificats, el seu ús queda restringit per a les tasques pròpies del Càrrec i pels usos inclosos al certificat.

#### **1.4.2.13 Requisits específics per als CESR i CESA**

Els CESR i els CESA no poden utilitzar-se per signar peticions d'emissió, renovació, suspensió o revocació de certificats CIC, ni per signar certificats de clau pública de cap tipus, ni signar llistes de revocació de certificats (LRC).

Els CESR i els CESA tampoc no poden utilitzar-se per signar missatges d'autenticació incomprensibles per al signant, en particular desafiaments de client SSL o TLS, excepte quan es combinin amb un CEI, i tampoc es poden utilitzar per rebre missatges xifrats, excepte quan es combinin amb un CEX i no s'emmagatzemi la clau privada.

#### **1.4.2.14 Requisits específics per al CEX**

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



#### **1.4.2.15 Requisits específics per al CDS**

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

#### **1.4.2.16 Requisits específics per al CDA**

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

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

#### **1.4.2.17 Requisits específics per al COS**

Sense estipulació.

### **1.5 Administració de la política**

#### **1.5.1 Organització que administra l'especificació**

Adreça Postal: CATCert - Agència Catalana de Certificació

Passatge de la Concepció, 11

08008 Barcelona.

Adreça web: <http://www.catcert.cat>

#### **1.5.2 Dades de contacte de l'organització**

Adreça Postal: CATCert - Agència Catalana de Certificació

Àrea d'Assessorament i Recerca

Passatge de la Concepció, 11

08008 Barcelona.

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

CATCert - Agència Catalana de Certificació

Àrea d'Assessorament i Recerca

Passatge de la Concepció, 11

08008 – Barcelona.

### 1.5.4 Procediment d'aprovació

El sistema documental i d'organització de l'Entitat de Certificació haurà de garantir, mitjançant l'existència i l'aplicació dels corresponents procediments, el correcte manteniment de la política de certificació i de les especificacions de servei relacionades amb ella.

Es preveuran, 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 política hauran de ser aprovades per CATCert, després de comprovar el compliment dels requisits establerts a les seccions corresponents d'aquesta política.

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

---

### 2.1 Directori de certificats

El servei de directori de certificats estarà disponible durant les 24 hores dels 7 dies de la setmana i, en cas de fallada del sistema fora de control de l'Entitat de Certificació, aquesta realitzarà els seus millors esforços perquè el servei es trobi disponible de nou en el termini establert a la secció corresponent i a la DPC aplicable.

### 2.2 Publicació d'informació de l'Entitat de Certificació

L'Entitat de Certificació publicarà les següents informacions<sup>3</sup>, en el 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.
- 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.

Tot canvi en les especificacions o condicions del servei serà comunicat als usuaris per l'Entitat de Certificació.

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

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

### 2.3 Freqüència de publicació

La informació de l'Entitat de Certificació es publicarà quan es trobi disponible i, en especial, de forma immediata quan s'emetin les mencions relatives a la vigència dels certificats.

Els canvis en la DPC es regiran per l'establert a la secció corresponent de la DPC.

La informació d'estat de revocació de certificats es publicarà d'acord amb l'establert a les seccions corresponents d'aquesta política.

Al cap de 15 (quinze) dies des de la publicació de la nova versió, es podrà retirar la referència al canvi de la pàgina principal i serà inserida en el directori.

Les versions antigues de la documentació seran conservades, per un període de 15 (quinze) anys per l'Entitat de Certificació, podent ser consultades, per causa raonada, pels interessats.

---

<sup>3</sup> TS 101 456: 7.3.5; TS 102042: 7.3.5

## 2.4 Control d'accés

L'Entitat de certificació no limitarà l'accés de lectura a les informacions establertes a la secció corresponent, però establirà 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<sup>4</sup>

L'Entitat de Certificació utilitzarà sistemes fiables per al Directori, de tal manera que<sup>5</sup>:

- 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 la persones que el signant hagi indicat.
  - Es pugui detectar qualsevol canvi tècnic que afecti els requisits de seguretat.

---

<sup>4</sup> TS 101 456: 7.3.6 j); TS 102042: 7.3.6 j)

<sup>5</sup> Llei 59/2003: 20.1g)

## 3. Identificació i autenticació

---

### 3.1 Gestió de noms<sup>6</sup>

En aquesta secció s'estableixen requisits relatius als procediments d'identificació i autenticació que s'han d'utilitzar durant el registre d'Entitats de Certificació Vinculades i subscriptors, incloent organitzacions i persones físiques, que ha de realitzar-se amb anterioritat a l'emissió i lliurament de certificats.

#### 3.1.1 Tipus de noms

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

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

#### 3.1.2 Significat dels noms

En certificats corresponents a persones físiques, la identificació del signant estarà formada pel seu nom i cognoms, més el seu DNI, o en el seu cas, un pseudònim que consti com a tal de manera inequívoca<sup>7</sup>.

En certificats corresponents a persones jurídiques, aquesta identificació es realitzarà per mitjà de la seva denominació o raó social, i el seu CIF<sup>8</sup>.

#### 3.1.3 Utilització d'anònims i pseudònims

No es poden utilitzar pseudònims per identificar una organització.

Els certificats personals, tant individuals com d'organització, i els d'entitat poden utilitzar pseudònims en lloc del nom vertader del posseïdor de la clau corresponent al certificat.

El pseudònim constarà com a tal de manera inequívoca<sup>9</sup>.

#### 3.1.4 Interpretació de formats de noms

Sense estipulació addicional.

---

<sup>6</sup> TS 101 456: 7.3.1

<sup>7</sup> Article 11.2.e) Llei 59/2003

<sup>8</sup> Article 11.2.e) Llei 59/2003

<sup>9</sup> Article 11.2.e) Llei 59/2003

### 3.1.5 Unicitat dels noms

Els noms dels subscriptors de certificats seran únics, per a cada servei de generació de certificats operat per una Entitat de Certificació Vinculada i per a cada tipus de certificat; és a dir, una persona podrà tenir al seu nom certificats de tipus diferents expedits per la mateixa Entitat de Certificació Vinculada.

També podrà tenir certificats al seu nom del mateix tipus expedits per diferents Entitats de Certificació Vinculades.

No es podrà tornar a assignar un nom de subscriptor que ja hagi estat ocupat, a un subscriptor diferent<sup>10</sup>.

### 3.1.6 Resolució de conflictes relatius a noms

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

L'Entitat de Certificació no haurà de determinar que un sol·licitant de certificats té dret sobre el nom que apareix en una sol·licitud de certificat.

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

L'Entitat de Certificació es reserva el dret de refusar una sol·licitud de certificat a causa de conflicte de nom.

En *certificats individuals*, els conflictes de noms de subscriptors que apareguin identificats als certificats amb el seu nom real se solucionen mitjançant la inclusió, en el nom diferenciat del certificat, de:

- En cas de nacionals espanyols, el DNI del subscriptor.  
V.gr.: (C) = ES; (SN) = DNI
- En cas d'estrangers amb algun tipus de vinculació amb Espanya, com pot ser la residència a territori espanyol, el NIE del subscriptor.  
V.gr.: francès (C) = ES; (SN) = NIE  
V.gr.: argentí (C) = ES; (SN) = NIE
- En cas d'estrangers nacionals d'Estats que són part de l'Acord Schengen i que no tenen el NIE, el document nacional d'identitat del país d'origen o de procedència o passaport vigent del subscriptor.  
V.gr.: italià (C) = IT; (SN) = IT-Document nacional d'identitat
- En cas d'estrangers nacionals d'Estats que no són part de l'Acord Schengen i que no tenen el NIE, el Passaport ordinari, diplomàtic, oficial o de servei, del subscriptor vàlidament expedit i en vigor.  
V.gr.: xinès (C) = CN; (SN) = CN-Passaport

<sup>10</sup> TS 101 456: 7.3.3 d); TS 102042: 7.3.3 d)

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

En *certificats d'organització*, els conflictes de noms de posseïdors de claus que apareguin identificats als certificats amb el seu nom real se solucionen mitjançant la inclusió, en el nom diferenciat del certificat, de:

- En cas que l'“Organizational Unit”, o subscriptor, del camp “Subject” estigui sotmès al Dret espanyol:
  - En cas de nacionals espanyols, el DNI del posseïdor de claus.  
V.gr.: (C) = ES; (SN) = DNI
  - En cas d'estrangers, amb algun tipus de vinculació amb Espanya, com pot ser la residència a territori espanyol, el NIE del posseïdor de claus.  
V.gr.: francès (C) = ES; (SN) = NIE  
V.gr.: argentí (C) = ES; (SN) = NIE
  - En cas d'estrangers nacionals d'Estats part de l'Acord Schengen i que no tenen el NIE, el DNI del país d'origen o de procedència o passaport vigent del posseïdor de claus.  
V.gr.: italià (C) = ES; (SN) = IT-Document nacional d'identitat
  - En cas d'estrangers nacionals d'Estats que no són part de l'Acord Schengen i que no tenen el NIE, el Passaport ordinari, diplomàtic, oficial o de servei del posseïdor de claus vàlidament expedit i en vigor.  
V.gr.: xinès (C) = ES; (SN) = CN-Passaport

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

  - Qualsevol altre identificador assignat al posseïdor de claus pel subscriptor.  
V.gr.: un número de col·legiat.
- En cas que l'“Organizational Unit”, o subscriptor, del “Subject” no estigui sotmès al dret espanyol, la semàntica del “SerialNumber” dependrà de la normativa aplicable conforme al “countryName” de l'Entitat.

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

Aquests criteris s'assenten tenint en compte que els diferents organismes de l'Administració Pública estatal, autonòmica o local, estableixen quins tipus d'identificacions consideren vàlides i respecte de quins tràmits són exigibles; per tant, en funció del certificat

en qüestió del que disposi l'interessat, podrà o no tramitar davant d'una determinada Administració Pública.

En aquest sentit, i en atenció als certificats de CATCert, podrien realitzar-se tot tipus de tràmits, doncs s'utilitza el NIF per identificar a la persona (posseïdor o subscriptor), amb els certificats següents:

- CPSR amb Càrrec
- CPI amb Càrrec
- idCAT
- idCAT-T
- CPISA
- CPISR
- CPISR amb Càrrec
- CPISR amb Càrrec per a Ús Concret
- CPISR Estudiant
- CPIXSA
- CPIXSA amb Càrrec
- CPX
- CPX amb Càrrec
- CPX Estudiant

No obstant, la present política limita l'ús a les tasques pròpies del càrrec per als següents certificats:

- CPSR amb Càrrec
- CPI amb Càrrec
- CPISR amb Càrrec
- CPISR amb Càrrec per a Ús Concret
- CPX amb Càrrec
- CPIXSA amb Càrrec

Amb la resta de certificats de CATCert, els quals utilitzen criteris diferents al DNI o al NIE per identificar al subscriptor o al posseïdor de claus, només podran realitzar-se determinats tràmits, en funció dels criteris establerts per l'òrgan competent de cada Administració Pública. Entre aquests certificats trobem:

- CPISR d'Estudiant Estranger
- CPX d'Estudiant Estranger
- CPISR d'Estranger amb Càrrec
- CPX d'Estranger amb Càrrec



- idCAT-CEX.

Referent al tractament de marques registrades cal veure l'apartat corresponent.

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

## 3.2 Validació inicial de la identitat

### 3.2.1 Prova de possessió de clau privada

Aquesta secció descriu els mètodes a utilitzar per demostrar que es posseeix la clau privada corresponent a la clau pública objecte de certificació<sup>11</sup>.

El mètode de demostració de possessió de la clau privada serà el PKCS #10, una altra prova criptogràfica equivalent o qualsevol mètode aprovat per l'Agència Catalana de Certificació.

Aquest requisit no s'aplica quan el parell de claus és generat per l'Entitat de Registre Local, 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 de lliurament i acceptació del dispositiu segur i del corresponent certificat i parell de claus emmagatzemades en el seu interior.

Ha d'assegurar-se que únicament el subscriptor de certificats individuals o que el posseïdor de claus de certificats d'organització o de certificats d'entitat, té únicament la clau de signatura.

### 3.2.2 Autenticació de la identitat d'una organització

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

#### 3.2.2.1 Entitats de Certificació Vinculades operades per terceres persones

L'Entitat de Certificació Arrel ha d'autenticar, amb caràcter previ a l'emissió i lliurament d'un certificat d'Entitat de Certificació Vinculada, la identitat d'aquesta i altres dades establertes a la secció corresponent.

Per tot això, l'Entitat de Certificació podrà utilitzar els següents mètodes:

- 1) Obtenció d'informació sobre l'organització, d'un proveïdor extern de serveis d'aquesta naturalesa.

---

<sup>11</sup> TS 101456: 7.3.1.j); TS 102042: 7.3.1.n)

- 2) Comprovació de documentació justificativa aportada pel sol·licitant. En aquest cas, es requerirà la presència física del representant de la futura Entitat de Certificació.

### 3.2.2.2 Entitats de Registre

L'Entitat de Certificació ha d'autenticar, amb caràcter previ a l'emissió i lliurament d'un certificat d'operador, per a qualsevol dels components d'una Entitat de Registre, la identitat de l'Entitat de Registre i de l'operador, establerts a la secció corresponent per a certificats d'organització.

Per tot això, l'Entitat de Certificació podrà utilitzar els següents mètodes:

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

### 3.2.2.3 Subscriptors de certificats

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

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

#### ***Requisits per a certificats de classe 2***

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

L'Entitat de Certificació podrà utilitzar les Entitats de Registre per a aquesta tasca.

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

- 1) Obtenció d'informació sobre l'organització d'un proveïdor extern de serveis d'aquesta naturalesa, a discreció de l'Entitat de Certificació, que prèviament haurà d'aprovar el proveïdor extern.
- 2) Comprovació de la documentació justificativa aportada pel sol·licitant, sobre els següents extrems<sup>12</sup> :
  - a) Nom legal complet de l'organització
  - b) Estat legal de l'organització
  - c) Número d'identificació fiscal

---

<sup>12</sup> TS 101 456: 7.3.1 e); TS 102 042: 7.3.1 g)

d) Dades d'identificació registral

Adicionalment a la comprovació que hagi de fer-se de l'organització responsable del servidor segur, es comprovarà:

- 1) L'existència del servidor
- 2) La titularitat del nom de domini provinent del registre corresponent
- 3) L'autorització per l'organització de l'emissió del certificat al servidor

### 3.2.3 Autenticació de la identitat d'una persona física

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

#### 3.2.3.1 Elements d'identificació requerits<sup>13</sup>

L'Entitat de Certificació establirà el número i els tipus de documents que siguin necessaris per acreditar la identitat del posseïdor de la clau, podent utilitzar els següents:

- 1) Document Nacional d'Identitat o Número d'Identificació d'Estrangers o, de forma equivalent, justificant de renovació o reemissió de DNI (o NIE) més un altre document acreditatiu de la identitat amb fotografia.
- 2) Passaport.
- 3) Qualsevol altre dels admesos en dret, sempre que contingui, almenys, la següent informació<sup>14</sup>:
  - a) Nom i cognoms de la persona
  - b) Lloc i data de naixement
  - c) Número d'identitat reconegut legalment
  - d) Altres atributs de la persona que hagin de constar al certificat.

#### 3.2.3.2 Validació dels elements d'identificació<sup>15</sup>

##### ***Requisits per a certificats de Classe 1***

La informació d'identificació de posseïdors de claus de certificats de classe 1 es validarà comparant la informació de la sol·licitud amb els registres interns de l'Entitat de Registre, que ha d'assegurar-se de la correcció de la informació a certificar.

---

<sup>13</sup> Article 13.1 Llei 59/2003

<sup>14</sup> TS 101 456:7.3.1 d); TS 102 042: 7.3.1 f)

<sup>15</sup> TS 101 456:7.3.1 c); TS 102 042: 7.3.1 d)

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

### ***Requisits per a certificats de Classe 2***

La informació d'identificació de subscriptors de certificats individuals, així com de posseïdors de claus de certificats d'organització, es realitza contrastant la informació de la sol·licitud amb la documentació aportada, electrònicament o en suport físic.

#### **3.2.3.3 Necessitat de presència personal<sup>16</sup>**

La identificació de la persona física que hagi d'obtenir un certificat reconegut podrà realitzar-se:

- Mitjançant la seva presència davant dels encarregats de verificar la seva identitat.
- Mitjançant el procediment que estableix la normativa administrativa, quan la presència es realitzi davant de les Administracions Públiques.

Es podria prescindir de la presència si la signatura continguda a la sol·licitud d'expedició d'un certificat ha estat legitimada notarialment<sup>17</sup>, i en els casos previstos per l'article 13.4 de la Llei 59/2003, de 19 de desembre. Però aquesta política no dóna suport a aquest mecanisme per la inexistència d'un procediment a l'efecte per part dels notaris.

En particular, es podrà prescindir de la presència personal si la sol·licitud d'expedició d'un certificat ha estat autenticada mitjançant l'ús d'un certificat electrònic de signatura electrònica reconeguda classificat per CATCert, sempre que es trobi vigent i que el sol·licitant declari que no han transcorregut més de cinc anys des de la identificació amb presència personal.

Abans de l'emissió i lliurament d'un certificat reconegut, l'Entitat de Certificació haurà de contrastar la identitat del subscriptor de certificats individuals o del posseïdor de claus mitjançant la presència física directa o indirecta d'aquest.

Durant aquest tràmit, que es pot diferir al moment de lliurament i acceptació del certificat o del dispositiu segur de creació de signatura, es realitzarà la validació de la identitat de la persona.

### ***Requisits específics per als CPSR i CESR***

Abans de l'emissió i lliurament d'un certificat CPSR o CESR, l'Entitat de Certificació haurà de contrastar la identitat del subscriptor de certificats individuals o del posseïdor de claus mitjançant la presència física directa o indirecta d'aquest.

---

<sup>16</sup> TS 101 456: 7.3.1 c)

<sup>17</sup> Article 13.1 Llei 59/2003

Durant aquest tràmit, que pot diferir-se al moment de lliurament i acceptació del certificat o del dispositiu segur de creació de signatura, es realitzarà la validació de la identitat de la persona.

### 3.2.3.4 Vinculació de la persona física amb una organització

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

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

#### ***Requisits per a certificats de classe 2***

Quan s'expedeixin certificats d'organització, l'Entitat de Certificació ha d'obtenir una acreditació documental de la vinculació de la persona física amb l'organització, mitjançant qualsevol mitjà admès en dret<sup>18</sup>.

L'Entitat de Certificació podrà utilitzar les Entitats de Registre per a aquesta tasca.

### 3.2.4 Informació de subscriptor no verificada

No aplicable.

## 3.3 Identificació i autenticació de sol·licituds de renovació

### 3.3.1 Validació per a la renovació rutinària de certificats<sup>19</sup>

Abans de renovar un certificat, l'Entitat de Certificació haurà de comprovar que la informació utilitzada per verificar la identitat i la resta de dades del subscriptor i del posseïdor de la clau continuen sent vàlides.

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

---

<sup>18</sup> TS 101 456: 7.3.1 e); TS 102 042: 7.3.1 g)

<sup>19</sup> TS 101 456: 7.3.2; TS 102 042: 7.3.2

### 3.3.2 Validació per a la renovació de certificats després de la revocació<sup>20</sup>

Abans de generar un certificat a un subscriptor el certificat del qual va ser revocat -sempre que la causa de la revocació hagi estat diferent del compromís de la clau privada- l'Entitat de Certificació haurà de comprovar que la informació utilitzada per verificar la identitat i la resta de dades del subscriptor i del posseïdor de la clau, continuen sent vàlides.

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

### 3.4 Identificació i autenticació de la sol·licitud de revocació<sup>21</sup>

L'Entitat de Certificació haurà d'autenticar les peticions i informes relatius a la revocació d'un certificat, comprovant que provenen d'una font autoritzada.

Les esmentades peticions i informes seran confirmats complint amb els procediments establerts en la Declaració de Pràctiques de Certificació de l'Entitat de Certificació.

### 3.5 Autenticació d'una petició de suspensió

El subscriptor s'identifica telefònicament davant de CATCert, donant un número que l'identifiqui (NIF) i contestant correctament a la pregunta de desafiament.

---

<sup>20</sup> TS 101 456: 7.3.2; TS 102 042: 7.3.2

<sup>21</sup> TS 101 456: 7.3.6 c); TS 102 042: 7.3.6 c)

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

Els següents requisits d'operació del cicle de vida dels certificats no són aplicables pels certificats de proves, que es regiran per l'estipulat a la DPC de l'Entitat de Certificació Vinculada que els emeti.

### 4.1 Sol·licitud d'emissió de certificat

#### 4.1.1 Legitimació per sol·licitar l'emissió

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

Abans de l'emissió i lliurament d'un certificat, ha d'existir una sol·licitud de certificat.

En cas que sol·licitant i subscriptor siguin entitats diferents, hi ha d'haver una autorització de l'Entitat de Certificació per realitzar la sol·licitud, que s'instrumentarà jurídicament. Podran existir els següents tipus d'autoritzacions:

1. Classe 1. Entitat de Registre davant de l'Entitat de Certificació, autoritzant personal propi.
2. Classe 2. Entitat de Registre davant de l'Entitat de Certificació, autoritzant personal relacionat amb el subscriptor (pot ser un treballador del subscriptor, o un representant extern, o fins i tot una entitat diferent).

Podran existir els següents tipus de sol·licituds:

1. Sol·licitud electrònica de certificat d'ofici (no conté clau pública, ni va signada digitalment)
2. Sol·licitud electrònica de certificat per part de l'interessat sense generació de claus (no conté clau pública, ni va signada digitalment)
3. Sol·licitud electrònica de certificat per part de l'interessat amb generació de claus (PKCS# 10 o mecanisme compatible, amb la clau pública de l'usuari i la seva signatura digital, per tal de demostrar la possessió de la clau privada, d'acord amb la secció corresponent de la present política de signatura).

##### 4.1.1.2 Requisits específics del CIC

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

##### 4.1.1.3 Requisits per a certificats personals, d'entitat i de dispositiu

#### *Requisits específics per a certificats de Classe 1*

Addicionalment a l'establert a la secció corresponent, l'Entitat de Certificació Vinculada haurà de rebre sol·licituds de certificats, si més no d'acord amb un dels següents casos:

- 1) Sol·licitud realitzada per una persona autoritzada per l'Entitat de Certificació Vinculada, en lloc del posseïdor de claus.

En aquest cas, hi ha d'haver un document, ja sigui en paper o en format electrònic, referent a la petició de certificats, realitzada per l'organització a l'Entitat de Certificació Vinculada, que inclourà la indicació de la persona o persones a autoritzar per a realitzar peticions.

Les dades de l'usuari final necessàries per a realitzar la sol·licitud podran provenir d'una base de dades de l'organització o, en el cas que l'usuari no sigui en aquesta base de dades, seran introduïdes manualment pel sol·licitant.

- 2) Sol·licitud realitzada pel futur posseïdor de claus, cas en el qual es poden presentar diverses circumstàncies:
  - Hi ha un document, ja sigui en paper o en format electrònic, de la petició del certificat.
  - El sol·licitant genera el seu parell de claus o acorda que se li generaran.
  - El sol·licitant ha generat el seu parell de claus, cas en el qual ha d'enviar la clau pública per a certificació i demostrar que té la clau privada.
  - El sol·licitant accepta un acord de subscriptor, el qual poden ser unes condicions d'ús.
  - Para solicitar un certificado puede usarse otro vigente, de acuerdo con lo establecido en el art. 13.4.b de la llei 59/2003.

### ***Requisits específics per a certificats de Classe 2***

Adicionalment a l'establert a la secció corresponent, l'Entitat de Certificació Vinculada haurà de rebre sol·licituds de certificats, si més no d'acord amb un dels següents casos:

- 1) Sol·licitud realitzada per una persona autoritzada per l'Entitat de Certificació Vinculada, en lloc del subscriptor, en cas de certificats individuals, o del posseïdor de claus en cas de certificats d'organització. En aquest cas, hi ha d'haver un document, ja sigui en paper o en format electrònic, referent a la petició de certificats realitzada per la futura entitat sol·licitant a l'Entitat de Certificació Vinculada que inclourà la indicació de la persona o persones a autoritzar per a realitzar peticions. Les dades de l'usuari final necessàries per a realitzar la sol·licitud seran introduïdes, en tot cas, pel sol·licitant.
- 2) Sol·licitud realitzada pel futur subscriptor, en cas de certificats individuals o pel futur posseïdor de claus, en cas de certificats d'organització, cas en el qual es poden presentar diverses circumstàncies:
  - Hi ha un document, ja sigui en paper o en format electrònic, de la petició del certificat.
  - El sol·licitant genera el seu parell de claus o acorda que se li generaran.
  - El sol·licitant ha generat el seu parell de claus, cas en el qual ha d'enviar la clau pública per a certificació i demostrar que té la clau privada.
  - El sol·licitant accepta un acord de subscriptor, el qual poden ser unes condicions d'ús.



## 4.1.2 Procediment d'alta; Responsabilitats

L'Entitat de Certificació Vinculada ha d'assegurar-se que les sol·licituds de certificats són completes, precises i estan degudament autoritzades<sup>22</sup>.

Abans de l'emissió i lliurament del certificat, l'Entitat de Certificació Vinculada informará el subscriptor, en cas de certificats individuals o al posseïdor de claus, en cas de certificats d'organització, dels termes i condicions aplicables al certificat<sup>23</sup>.

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

L'esmentada informació es comunicarà en suport perdurable, en paper o electrònicament i en llenguatge fàcilment comprensible<sup>24</sup>.

A la sol·licitud es podrà acompanyar documentació justificativa de la identitat del subscriptor i altres circumstàncies, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització o d'entitat, d'acord amb l'establert a la secció corresponent d'aquesta política de certificats.

També es podrà acompanyar una adreça física, o altres dades, que permetin contactar amb el subscriptor, en cas de certificats individuals, o al posseïdor de claus, en cas de certificats d'organització o d'entitat<sup>25</sup>.

## 4.2 Processament de la sol·licitud de certificació

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

Una vegada hagi tingut lloc una petició de certificat, l'Entitat de Certificació ha de verificar la informació proporcionada, conforme a la secció corresponent d'aquesta política.

Si la informació no és correcta, l'Entitat de Certificació ha de denegar la petició. En cas que les dades es verifiquin correctament l'Entitat de Certificació aprovarà el certificat.

### 4.2.2 Requisits específics per al 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 necessària fiabilitat dels seus serveis<sup>26</sup>.

CATCert comprovarà, en el procés d'admissió de l'Entitat de Certificació, els següents aspectes:

---

<sup>22</sup> TS 101 456: 7.3.1; TS 102 042: 7.3.1

<sup>23</sup> TS 101 456: 7.3.1 a); TS 102 042: 7.3.1 a)

<sup>24</sup> TS 101 456: 7.3.1 b); TS 102 042: 7.3.1 c)

<sup>25</sup> TS 101 456: 7.3.1 f); TS 102 042: 7.3.1 j)

<sup>26</sup> Llei 59/2003: Article 20.1 a); TS 101 456: 7.5; TS 102 042: 7.5

- Que les polítiques i procediments operats per l'Entitat de Certificació no són discriminatoris<sup>27</sup>.
- Que l'Entitat de Certificació oferirà els seus serveis a tots els sol·licitants les activitats dels quals entrin en l'àmbit d'operació declarada<sup>28</sup> en la seva DPC, d'acord amb l'establert a la secció 1.3 d'aquesta política.
- Que l'Entitat de Certificació és una entitat legal<sup>29</sup>, d'acord amb l'establert a la secció 1.3.1 d'aquesta política, dada que serà autenticada d'acord amb l'establert a la secció corresponent d'aquesta política.
- Que l'Entitat de Certificació disposa de sistemes de gestió de la qualitat i la seguretat adequats per a la prestació del servei<sup>30</sup>, dada que serà comprovada a l'auditoria de conformitat prevista a la secció 8 d'aquesta política.
- 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<sup>31</sup>.
- Que l'Entitat de Certificació compleix els requisits de capacitat financera establerts a la secció 9.2 d'aquesta política<sup>32</sup>.
- Que l'Entitat de Certificació compleix els requisits relatius als procediments de resolució de disputes, establerts a la secció 9.13 d'aquesta política<sup>33</sup>.
- Que l'Entitat de Certificació ha documentat adequadament les relacions jurídiques en virtut de les quals externalitza part o la totalitat dels seus serveis<sup>34</sup>.

### 4.2.3 Requisits per als certificats personals

L'Entitat de Certificació haurà de:

- Utilitzar un procediment de generació de certificats que vinculi de forma segura el certificat amb la informació de registre, incloent la clau pública certificada<sup>35</sup>.
- En cas que l'Entitat de Certificació generi el parell de claus, utilitzar un procediment de generació de certificats vinculat de forma segura amb el procediment de generació de claus, i que la clau privada sigui lliurada de forma segura al

---

<sup>27</sup> TS 101 456: 7.5 a); TS 102 042: 7.5 a)

<sup>28</sup> TS 101 456: 7.5 b); TS 102 042: 7.5 b)

<sup>29</sup> TS 101 456: 7.5 c); TS 102 042: 7.5 c)

<sup>30</sup> TS 101 456: 7.5 d); TS 102 042: 7.5 d)

<sup>31</sup> Llei 59/2003: Article 20.1 c); TS 101 456: 7.5 g); TS 102 042: 7.5 g)

<sup>32</sup> TS 101 456: 7.5 f); TS 102 042: 7.5 f)

<sup>33</sup> TS 101 456: 7.5 h); TS 102 042: 7.5 h)

<sup>34</sup> TS 101 456: 7.5 i); TS 102 042: 7.5 i)

<sup>35</sup> TS 101 456: 7.3.3 b); TS 102042: 7.3.3 b)

subscriptor, en cas de certificats individuals, o al posseïdor de claus, en cas de certificats d'organització<sup>36</sup> o d'entitat.

- Protegir el secret i la integritat de les dades de registre, especialment en cas que siguin intercanviats amb el subscriptor, en cas de certificats individuals, amb el posseïdor de claus, en cas de certificats d'organització o d'entitat, o amb el tercer sol·licitant, en el seu cas<sup>37</sup>.

#### 4.2.3.1 Requisits específics per als certificats personals

Adicionalment, l'Entitat de Certificació haurà de:

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

- Garantir la data i l'hora en què es va expedir un certificat<sup>38</sup>.

- En cas que l'Entitat de Certificació aporti el seu dispositiu segur de creació de signatura, utilitzar un procediment de gestió de dispositius segurs de creació de signatura que assegurí que l'esmentat dispositiu és lliurat de forma segura al subscriptor, en cas de certificats individuals, o al posseïdor de claus, en cas de certificats d'organització<sup>39</sup>.

- Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, en el seu cas, criptogràfica dels processos de certificació a què serveixen de suport<sup>40</sup>.

- Assegurar-se que el certificat és emès per sistemes que utilitzin protecció contra falsificació i, en cas que l'Entitat de Certificació generi claus privades, que garanteixin el secret de les claus durant el procés de generació de les esmentades claus<sup>41</sup>.

#### 4.2.4 Requisits per als certificats d'entitat

Adicionalment, l'Entitat de Certificació haurà de:

- Incloure al certificat les informacions establertes a l'article 11.2 de la Llei 59/2003, d'acord amb l'establert a la secció 7 d'aquesta política.

- Garantir la data i l'hora en què es va expedir un certificat<sup>42</sup>.

---

<sup>36</sup> TS 101 456: 7.3.3 c); TS 102042: 7.3.3 c)

<sup>37</sup> TS 101 456: 7.3.3 e); TS 102042: 7.3.3 e)

<sup>38</sup> Llei 59/2003: Art. 20.1 b)

<sup>39</sup> TS 101 456: 7.3.3 c); TS 102042: 7.3.3 c)

<sup>40</sup> Llei 59/2003: Art. 20.1

<sup>41</sup> TS 101 456: 7.3.3, amb referència a D 99/93: Annex II g);

<sup>42</sup> Llei 59/2003: Art. 20.1 b)

- En cas que l'Entitat de Certificació aportí el dispositiu segur de creació de signatura, utilitzar un procediment de gestió de dispositius segurs de creació de signatura que assegurí que l'esmentat dispositiu és lliurat de forma segura al responsable de la custòdia de les claus<sup>43</sup>.
- Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, en el seu cas, criptogràfica dels processos de certificació a què serveixen de suport<sup>44</sup>.
- Assegurar-se que el certificat és emès per sistemes que utilitzin protecció contra falsificació i, en cas que l'Entitat de Certificació generi claus privades, que garanteixin el secret de les claus durant el procés de generació de les esmentades claus<sup>45</sup>.

## 4.2.5 Requisits per als certificats de dispositiu

Una vegada aprovada la sol·licitud de certificat de servidor segur, l'Entitat de Certificació, o l'Entitat de Registre autoritzada, es posarà en contacte amb el responsable de la instal·lació del certificat, per determinar el mecanisme de tramesa de la clau pública a certificar, d'acord amb l'establert a la secció corresponent.

Després de la recepció, en condicions de seguretat, de la clau pública, es procedirà a l'emissió del certificat i al seu lliurament.

## 4.3 Emissió de certificat

### 4.3.1 Accions de l'Entitat de Certificació durant el procés d'emissió

Després de l'aprovació de la sol·licitud de certificació es procedirà a l'emissió del certificat de forma segura<sup>46</sup>, i es posarà el certificat a disposició del subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització o d'entitat, per a l'acceptació d'aquest, d'acord amb l'establert a la secció corresponent<sup>47</sup>.

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

L'Entitat de Certificació haurà de:

- a. Utilitzar un procediment de generació de certificats que vinculi de forma segura el certificat amb la informació de registre, incloent la clau pública certificada<sup>48</sup>.

---

<sup>43</sup> TS 101 456: 7.3.3 c); TS 102042: 7.3.3 c)

<sup>44</sup> Llei 59/2003: Art. 20.1 d)

<sup>45</sup> TS 101 456: 7.3.3, amb referència a D 99/93: Annex II g);

<sup>46</sup> TS 101 456: 7.3.3

<sup>47</sup> TS 101 456: 7.3.5 a)

<sup>48</sup> TS 101 456: 7.3.3 b)

- b. En cas que l'Entitat de Certificació generi el parell de claus, utilitzar un procediment de generació de certificats vinculat de forma segura amb el procediment de generació de claus i, que la clau privada és lliurada de forma segura al subscriptor, en cas de certificats individuals, o al posseïdor de claus en cas de certificats d'organització o d'entitat.<sup>49</sup>
- c. Protegir la confidencialitat i integritat de les dades de registre, especialment en cas que siguin intercanviades amb el subscriptor, en cas de certificats individuals, amb el posseïdor de claus, en cas de certificats d'organització o d'entitat, o amb el tercer sol·licitant, en el seu cas<sup>50</sup>.

Adicionalment a l'establert a la secció corresponent, l'Entitat de Certificació haurà de:

- a. Incloure al certificat les informacions establertes a l'article 11.2 de la Llei 59/2003, d'acord amb l'establert a la secció corresponent d'aquesta política.
- b. Indicar la data i l'hora en les quals es va expedir un certificat<sup>51</sup>.
- c. En cas que l'Entitat de Certificació aporti el dispositiu segur de creació de signatura, utilitzar un procediment de gestió de dispositius segurs de creació de signatura que assegurí que aquest dispositiu és lliurat de forma segura al subscriptor, en cas de certificats individuals, o al posseïdor de claus, en cas de certificats d'organització o d'entitat<sup>52</sup>.
- d. Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, en el seu cas, criptogràfica dels processos de certificació a què serveixen de suport<sup>53</sup>.
- e. Prendre mesures contra la falsificació de certificats i, en cas que l'Entitat de Certificació Vinculada generi claus privades, que garanteixin el secret de les claus durant el procés de generació d'aquestes claus<sup>54</sup>.

### 4.3.2 Notificació de l'emissió al subscriptor

L'Entitat de Certificació haurà de notificar al sol·licitant l'aprovació o denegació de la sol·licitud.

També es notificarà al subscriptor, en cas de certificats individuals, o al futur posseïdor de claus, en cas de certificats d'organització o d'entitat, que s'ha creat el certificat, es troba disponible i la forma d'obtenir-lo.

---

<sup>49</sup> TS 101 456: 7.3.3 c)

<sup>50</sup> TS 101 456: 7.3.3 e)

<sup>51</sup> Art. 20,1,b) Llei 59/2003

<sup>52</sup> TS 101 456: 7.3.3 c)

<sup>53</sup> Llei 59/2003: 20.1.d)

<sup>54</sup> TS 101 456: 7.3.3, amb referència a D 99/93: Annex II g); Art. 20,1,e) Llei 59/2003

## 4.4 Acceptació del certificat

### 4.4.1 Responsabilitats del Prestador de Serveis de Certificació

L'Entitat de Certificació haurà de:

- Si no ho ha fet abans, i quan resulti necessari, acreditar la identitat del subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització o d'entitat, d'acord amb l'establert a les seccions corresponents d'aquesta política.
- Proporcionar al subscriptor, en cas de certificats individuals, o al futur posseïdor de claus, en cas de certificats d'organització o d'entitat, accés al certificat<sup>55</sup>.
- Lliurar, en el seu cas, el dispositiu criptogràfic de signatura, verificació de signatura, xifrat o desxifrat.
- En cas de certificats d'organització i d'entitat, lliurar el posseïdor de claus, un full de lliurament del certificat (i, en el seu cas, del dispositiu criptogràfic indicat en l'apartat anterior), amb els següents continguts mínims:
  - Informació bàsica sobre la política i ús del certificat, incloent especialment informació sobre l'Entitat de Certificació Vinculada i de la Declaració de Pràctiques de Certificació aplicable, així com de 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 podrà acceptar mitjançant la signatura del full de lliurament de subscriptor i, quan sigui necessari, del full de posseïdor de claus.

També es podrà acceptar el certificat en suport programari mitjançant un mecanisme telemàtic.

---

<sup>55</sup> TS 101 456: 7.3.5 a); TS 102042: 7.3.5 a)

### 4.4.3 Publicació del certificat

Els certificats de classe 1 es podran publicar en tot cas, sense el consentiment previ dels posseïdors de claus, mentre que la publicació dels certificats de classe 2 requerirà sempre el consentiment dels subscriptors<sup>56</sup>.

### 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 subscriptors

Els certificats s'utilitzaran 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'hauran d'utilitzar únicament d'acord amb la llei aplicable, especialment tenint en compte les restriccions d'importació i exportació existents en cada moment.

L'extensió Key Usage s'utilitzarà 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.

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 ha estat fabricada ni pot estar controlada per les Entitats de Certificació.

Obligacions per part del subscriptor:

Utilitzar el parell de claus exclusivament per a signatures electròniques i d'acord amb qualsevol altres limitacions que li siguin notificades<sup>57</sup>.

Ser especialment diligent en la custòdia de la seva clau privada i del seu dispositiu segur de creació de signatura, amb la finalitat d'evitar usos no autoritzats.<sup>58</sup>

Si el subscriptor genera les seves pròpies claus, s'obliga a:

- Generar les seves claus de subscriptor utilitzant un algoritme reconegut com a acceptable per a la signatura electrònica reconeguda<sup>59</sup>
- Crear les claus dins del dispositiu segur de creació de signatura<sup>60</sup>
- Utilitzar longituds i algoritmes de clau reconeguts com a acceptables per a la signatura electrònica reconeguda.<sup>61</sup>

---

<sup>56</sup> Llei 59/2003: Art. 17.2

<sup>57</sup> TS 101456: 6.2.b)

<sup>58</sup> TS 101456: 6.2.c), més estricta, i extensió al dispositiu segur de creació de firma.

<sup>59</sup> TS 101456: 6.2.d) primer

<sup>60</sup> TS 101456: 6.2.f)

<sup>61</sup> TS 101456: 6.2.d) segon



## 4.5.2 Ús pel tercer que confia en certificats

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

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

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

## 4.6 Renovació de certificats sense renovació de claus

Quan se sol·liciti la renovació d'un certificat sense renovació del parell de claus, l'Entitat de Registre haurà de comprovar que aquest parell de claus encara és criptogràficament fiable.

En cas que així es consideri, llavors l'Entitat de Registre haurà de verificar que les dades de registre continuen sent vàlides i, si alguna dada ha canviat aquesta ha de ser verificada, guardada i el subscriptor ha d'estar d'acord amb ella, així com s'especifica a la secció corresponent d'aquesta política<sup>62</sup>.

Si les condicions jurídiques de prestació del servei han variat des de l'emissió del certificat, serà necessari que l'Entitat de Certificació o, quan convingui, l'Entitat de Registre, hauran d'informar d'aquest fet al sol·licitant<sup>63</sup>.

### 4.6.1 Requisits específics per als certificats d'infraestructura

Els certificats d'infraestructura no es poden renovar, en cap cas, sense procedir també a la renovació de claus.

### 4.6.2 Requisits específics per als certificats de signatura electrònica reconeguda

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

---

<sup>62</sup> TS 101 456: 7.3.2 a) i c); TS 102 042: 7.3.2 a) i c)

<sup>63</sup> TS 101 456: 7.3.2 b); TS 102 042: 7.3.2 b)

### 4.6.3 Requisits específics per a la resta de certificats personals

El procediment aplicable a la renovació sense renovació de claus d'aquests certificats podrà basar-se en l'existència prèvia d'un certificat vigent, sempre que el parell de claus d'aquest certificat sigui criptogràficament fiable per al nou termini de vigència del nou certificat, i que no existeixi la sospita del compromís de la clau privada del subscriptor o del posseïdor de claus<sup>64</sup>.

## 4.7 Renovació de certificat amb renovació de claus

Quan se sol·liciti la renovació d'un certificat amb renovació del parell de claus, l'Entitat de Registre haurà de verificar que les dades de registre continuen sent vàlides i, si alguna dada ha canviat, aquesta ha de ser verificada, guardada i el subscriptor ha d'estar d'acord amb ella, de la forma com s'especifica a la secció corresponent d'aquesta política<sup>65</sup>.

Si les condicions jurídiques de prestació del servei han variat des de l'emissió del certificat, serà necessari que l'Entitat de Certificació o bé l'Entitat de Registre informin d'aquest fet al sol·licitant<sup>66</sup>.

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

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

Per a certificats en clau, el subscriptor ha de dirigir-se a les oficines de l'Entitat de Registre.

## 4.8 Renovació telemàtica

CATCert permet la renovació telemàtica de certificats digitals a partir d'una autenticació segura i la corresponent signatura electrònica del full de lliurament del nou certificat, realitzada amb el certificat a renovar dins dels seus dos darrers mesos de vigència.

## 4.9 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

---

<sup>64</sup> TS 101 456: 7.3.2 d); TS 102 042: 7.3.2 d)

<sup>65</sup> TS 101 456: 7.3.2 a) i c); TS 102 042: 7.3.2 a) i c)

<sup>66</sup> TS 101 456: 7.3.2 b); TS 102 042: 7.3.2 b)

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.

## 4.10 Revocació i suspensió de certificats

L'Entitat de Certificació haurà de detallar en la seva Declaració de Pràctiques de Certificació els següents aspectes<sup>67</sup> :

- a. Qui pot sol·licitar la revocació i suspensió
- b. Com es remetrà la sol·licitud
- c. Els requisits de confirmació de sol·licituds de revocació i suspensió
- d. Les causes de suspensió i revocació
- e. Els mecanismes utilitzats per distribuir la informació d'estat de revocació
- f. El màxim retard entre la recepció de la sol·licitud i la disponibilitat per a verificadors del canvi de l'estat de revocació, que no podrà superar en cap cas el termini d'un dia.

### 4.10.1 Causes de revocació de certificats

Una Entitat de Certificació podrà revocar un certificat per la concurrència d'alguna de les següents causes:

#### 1. Circumstàncies que afectin la informació continguda al certificat<sup>68</sup>

- Modificació d'alguna de les dades contingudes al certificat que no permeten fer una modificació.
- Descobriment que alguna de les dades aportades a la sol·licitud de certificat és incorrecta, així com l'alteració o modificació de les circumstàncies verificades per a l'expedició del certificat.
- Descobriment que alguna de les dades contingudes al certificat és incorrecte.

#### 2. Circumstàncies que afecten la seguretat de la clau o del certificat

- Compromís de la clau privada o de la infraestructura o sistemes de l'Entitat de Certificació que va emetre el certificat, sempre que afecti la fiabilitat dels certificats emesos a partir d'aquest incident.
- Infracció, per part de l'Entitat de Certificació, dels requisits previstos en els procediments de gestió de certificats, establerts en la DPC de l'Entitat de Certificació.

<sup>67</sup> TS 101 456: 7.3.6 a); TS 102042: 7.3.6 a)

<sup>68</sup> Llei 59/2003: Art. 8.1.g)

- Compromís o sospita de compromís de la seguretat de la clau o del certificat del subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització o d'entitat<sup>69</sup>.
- Accés o utilització no autoritzat, per part d'un tercer, de la clau privada del subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització o d'entitat<sup>70</sup>.
- L'ús irregular del certificat pel subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització o d'entitat, o falta de diligència en la custòdia de la clau privada.

### 3. Circumstàncies que afecten la seguretat del dispositiu criptogràfic

- Compromís o sospita de compromís de la seguretat del dispositiu criptogràfic.
- Pèrdua o inutilització per danys del dispositiu criptogràfic.
- Accés no autoritzat, per part d'un tercer, a les dades d'activació del subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització o d'entitat.

### 4. Circumstàncies que afecten el subscriptor o el posseïdor de claus

- Acabament de la relació entre Entitat de Certificació Vinculada i el subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització o d'entitat.
- Modificació o extinció de la relació jurídica subjacent o causa que va provocar l'emissió del certificat al subscriptor, en cas de certificats individuals, o al posseïdor de claus, en cas de certificats d'organització o d'entitat.
- Infracció per part del sol·licitant del certificat dels requisits preestablerts per a la sol·licitud d'aquest.
- Infracció per part del subscriptor, en cas de certificats individuals, del posseïdor de claus, en cas de certificats d'organització o d'entitat, de les seves obligacions, responsabilitats i garanties, establertes a l'instrument jurídic corresponent o en la Declaració de Pràctiques de Certificació de l'Entitat de Certificació Vinculada que li va emetre el certificat.
- La incapacitat sobrevinguda o la mort del subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització o d'entitat<sup>71</sup>.
- En cas de certificats d'organització, l'extinció de la persona jurídica subscriptora del certificat<sup>72</sup>, així com la finalitat de l'autorització del subscriptor al posseïdor o l'acabament de la relació entre subscriptor i posseïdor de claus.

<sup>69</sup> Llei 59/2003: Art. 8.1.c)

<sup>70</sup> Llei 59/2003: Art. 8.1 c)

<sup>71</sup> Llei 59/2003: Art. 8.1 i)

<sup>72</sup> Llei 59/2003: Art. 8.1 i)

- Sol·licitud del subscriptor de revocació del certificat, d'acord amb l'establert a la secció 3.4 d'aquesta política.

#### 5. Altres circumstàncies

La suspensió del certificat digital per un període superior a 120 dies.

- La finalització de prestació de serveis per part de CATCert, d'acord amb el que estableix aquesta Política General de Certificació.
- Resolució judicial o administrativa que ho ordeni (Art. 8.1 de la Llei 59/2003, de signatura electrònica).

Si l'entitat a la què es dirigeix la sol·licitud de revocació no disposa de tota la informació necessària per determinar la revocació d'un certificat, però té indicis del seu compromís, pot decidir la suspensió.

En aquest cas es considerarà que les actuacions realitzades durant el període de suspensió no són vàlides, sempre que el certificat finalment sigui revocat. Seran vàlides si s'aixeca la suspensió (habilitació) i el certificat torna a passar a la situació de vàlid.

L'instrument jurídic que vincula a l'Entitat de Certificació Vinculada amb el subscriptor establirà que el subscriptor haurà de sol·licitar la revocació del certificat en cas de tenir coneixement d'alguna de les circumstàncies indicades anteriorment.

### 4.10.2 Legitimació per sol·licitar la revocació

Podran sol·licitar la revocació d'un certificat:

- En cas de certificats individuals, el subscriptor a nom del qual va ser emès el certificat.
- En cas de certificats d'organització, un representant autoritzat pel subscriptor o el posseïdor de claus.
- En cas de certificats d'entitat, un representant autoritzat pel subscriptor o el responsable de la custòdia de les claus.
- L'Entitat de Registre que va sol·licitar l'emissió del certificat.

### 4.10.3 Procediments de sol·licitud de revocació

L'Entitat de Certificació haurà de tenir en compte les següents regles:

L'entitat que necessiti revocar un certificat ha de sol·licitar-ho a l'Entitat de Certificació Vinculada o, en el seu cas, a l'Entitat de Registre que va aprovar la sol·licitud de certificació, comprensiva de la següent informació:

- Data de sol·licitud de la revocació
- Identitat del subscriptor
- Raó detallada per a la petició de revocació
- Nom i títol de la persona que demana la revocació

- Informació de contacte de la persona que demana la revocació

En aquells casos en els quals es requereixi revocació immediata del certificat, es podrà realitzar una crida o enviar un correu electrònic a l'Entitat de Certificació Vinculada o, en el seu cas, a l'Entitat de Registre.

La sol·licitud ha d'estar autenticada, pel seu destinatari, d'acord amb els requisits establerts a la secció corresponent d'aquesta política, abans de procedir a la revocació<sup>73</sup>.

En cas que el destinatari de la sol·licitud fos l'Entitat de Registre, una vegada autenticada podrà revocar directament el certificat o remetre una sol·licitud en aquest sentit a l'Entitat de Certificació Vinculada.

La sol·licitud de revocació serà processada a la seva recepció<sup>74</sup>.

S'haurà d'informar el subscriptor i, en el seu cas, el posseïdor de claus sobre el canvi d'estat del certificat revocat<sup>75</sup>.

L'Entitat de Certificació Vinculada no podrà reactivar el certificat, una vegada revocat<sup>76</sup>.

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

#### **4.10.4 Termini temporal de sol·licitud de revocació**

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

#### **4.10.5 Termini màxim de processament de la sol·licitud de revocació**

La sol·licitud de revocació serà processada en el mínim termini possible, sempre dins dels horaris d'oficina de l'Entitat de Certificació<sup>77</sup>.

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

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

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

---

<sup>73</sup> TS 101 456: 7.3.6. c); TS 102042: 7.3.6 c)

<sup>74</sup> TS 101 456: 7.3.6. b); TS 102042: 7.3.6 b)

<sup>75</sup> TS 101 456: 7.3.6. e); TS 102042: 7.3.6 e)

<sup>76</sup> TS 101 456: 7.3.6. f); TS 102042: 7.3.6 f)

<sup>77</sup> Llei 59/2003: Art. 10

Un mètode pel qual es pot verificar l'estat dels certificats és consultant la LRC més recent emesa per l'Entitat de Certificació que va emetre el certificat en què es desitja confiar.

L'Entitat de Certificació haurà de subministrar informació als verificadors sobre com i on trobar la LRC corresponent.

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

##### **4.10.7.1 Requisits específics del CIC**

L'Entitat de Certificació Arrel o entitat de certificació que expedeixi certificats d'entitat de certificació haurà d'emetre una LRC immediatament després de la revocació d'una Entitat de Certificació de la jerarquia.

En tot cas, emetrà una LRC cada 12 mesos com a màxim.

##### **4.10.7.2 Requisits per als certificats personals, d'entitat, de dispositiu i d'objecte**

L'Entitat de Certificació Vinculada haurà d'emetre una LRC almenys cada 24 hores<sup>78</sup>.

S'haurà d'indicar en la LRC el moment programat d'emissió d'una nova LRC, si bé es podrà emetre una LRC abans del termini indicat en la LRC anterior<sup>79</sup>.

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

#### **4.10.8 Període màxim de publicació de LRCs**

Les LRCs seran publicades immediatament al web de CATCert (<http://www.catcert.cat/>).

#### **4.10.9 Disponibilitat de serveis de comprovació d'estat de certificats**

De forma alternativa, els verificadors podran consultar els certificats publicats en el directori de l'Entitat de Certificació Vinculada, a través d'una interfície web.

---

<sup>78</sup> TS 101 456: 7.3.6 g); TS 102042: 7.3.6 g)

<sup>79</sup> TS 101 456: 7.3.6 g); TS 102042: 7.3.6 h)



#### **4.10.10 Obligació de consulta de serveis de comprovació d'estat de certificats**

El verificador que no utilitzi la LRC per comprovar la validesa d'un certificat, haurà d'utilitzar el directori de l'Entitat de Certificació Vinculada per a això.

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

Una forma per la qual es pot verificar l'estat dels certificats és consultant la LRC més recent emesa per l'Entitat de Certificació Vinculada que va emetre el certificat en què es desitja confiar.

L'Entitat de Certificació Vinculada haurà de subministrar informació als verificadors referent a com i on trobar la LRC corresponent.

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

Es podran establir altres formes per informar sobre la revocació dels certificats, que s'hauran de detallar en la DPC de l'Entitat de Certificació Vinculada. CATCert permet consultar l'estat de vigència dels certificats mitjançant el protocol OCSP.

#### **4.10.12 Requeriments especials en cas de compromís de la clau privada**

El compromís de la clau privada d'una Entitat de Certificació Vinculada serà notificat, en la mesura del possible, a tots els participants en la jerarquia pública de certificació de Catalunya, mitjançant el directori de CATCert.

#### **4.10.13 Causes de suspensió de certificats**

L'Entitat de Certificació Vinculada podrà suspendre un certificat en els següents casos:

- Si el subscriptor no utilitzés el certificat durant un període prolongat de temps, conegut prèviament.
- Si se sospita el compromís d'una clau, fins que aquest sigui confirmat. En aquest segon cas, l'Entitat de Certificació Vinculada ha d'assegurar-se que el certificat no està suspès durant més temps del necessari per confirmar el seu compromís.

#### **4.10.14 Qui pot sol·licitar la suspensió**

Podran sol·licitar la suspensió d'un certificat:

- En cas de certificats individuals, el subscriptor a nom del qual va ser emès el certificat.
- En cas de certificats d'organització, un representant autoritzat pel subscriptor o el posseïdor de claus.

- En cas de certificats d'entitat, un representant autoritzat del subscriptor o el responsable de la custòdia de les claus
- L'Entitat de Registre que va sol·licitar l'emissió del certificat.

#### **4.10.15 Procediments de petició de suspensió**

En cas de suspensió pel subscriptor o, en el seu cas, posseïdor de claus, haurà de disposar d'un certificat vàlid, per autenticar-se davant de l'Entitat de Certificació Vinculada o, en el seu cas, l'Entitat de Registre.

Si no disposa de certificat, es dirigirà a una Entitat de Certificació Vinculada o, en el seu cas, a una Entitat de Registre per instar la suspensió.

L'Entitat de Certificació Vinculada ha de determinar en la seva Declaració de Pràctiques de Certificació els procediments i mecanismes d'accés als sistemes de suspensió.

#### **4.10.16 Termini màxim de suspensió**

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

#### **4.10.17 Habilitació d'un certificat suspès**

El subscriptor podrà habilitar el certificat que roman suspès, personant-se i identificant-se davant l'Entitat de Certificació Virtual o en el seu cas 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.

### **4.11 Serveis de comprovació d'estat de certificats**

#### **4.11.1 Característiques d'operació dels serveis**

Les LRC seran descarregades des del directori de l'Entitat de Certificació Vinculada i seran instal·lades pels verificadors.

De forma alternativa, els verificadors podran consultar els certificats publicats en el directori de l'Entitat de Certificació Vinculada, a través d'una interfície web.

#### **4.11.2 Disponibilitat dels serveis**

Els sistemes de distribució de LRCs i de consulta en línia de l'estat dels certificats hauran d'estar disponibles les 24 hores dels 7 dies de la setmana<sup>80</sup>.

En cas de fallada dels sistemes de comprovació d'estat de certificats per causes fora del control de l'Entitat de Certificació, aquesta haurà de realitzar els seus millors esforços per

---

<sup>80</sup> TS 101 456: 7.3.6 i); TS 102042: 7.3.6 i)

assegurar que aquest servei es manté inactiu el mínim temps possible. L'Entitat de Certificació detallarà en la seva DPC el període màxim de temps en què el servei haurà de tornar a operar<sup>81</sup>.

L'Entitat de Certificació haurà de subministrar informació als verificadors sobre el funcionament del servei d'informació d'estat de certificats.

### 4.11.3 Altres funcions dels serveis

Sense estipulació addicional.

## 4.12 Finalització de la subscripció

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

## 4.13 Dipòsit i recuperació de claus

### 4.13.1 Política i pràctiques de dipòsit i recuperació de claus

L'Entitat de Certificació haurà de detallar en la seva DPC els següents aspectes:

- a. Qui pot sol·licitar el dipòsit i la recuperació de claus
- b. Com es remetrà la sol·licitud
- c. Els requisits de confirmació de sol·licituds
- d. Els mecanismes utilitzats per dipositar i recuperar claus

### 4.13.2 Política i pràctiques d'encapsulament i recuperació de claus de sessió

Sense estipulació addicional.

---

<sup>81</sup> TS 101 456: 7.3.6 i); TS 102042: 7.3.6 i)

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

---

### 5.1 Controls de seguretat física

L'Entitat de Certificació ha de disposar d'instal·lacions que protegeixin físicament la prestació, almenys, dels serveis de generació de certificats, de dispositius criptogràfics i de gestió de revocació i del compromís causat per l'accés no autoritzat als sistemes o a les dades.<sup>82</sup>

La protecció física s'aconseguirà mitjançant la creació de perímetres de seguretat clarament definits al voltant dels serveis de generació de certificats, de dispositius criptogràfics i de gestió de revocació. La part de les instal·lacions compartides amb altres organitzacions ha de trobar-se fora d'aquests perímetres.<sup>83</sup>

L'Entitat de Certificació establirà controls de seguretat física i ambiental per protegir els recursos de les instal·lacions on es trobin els sistemes, així com 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 establirà prescripcions per a les següents contingències<sup>84</sup>:

- Controls d'accés físic
- Protecció davant de desastres naturals
- Mesures de protecció davant d'incendis
- Decisió dels sistemes de suport (energia elèctrica, telecomunicacions, etc.)
- Demolició de l'estructura
- Inundacions
- Protecció antirobatori
- Conformitat i entrada no autoritzada
- Recuperació del desastre
- Sortida no autoritzada d'equipaments, informacions, suports i aplicacions relatives a components utilitzats per als serveis de l'Entitat de Certificació<sup>85</sup>.

#### 5.1.1 Localització i construcció de les instal·lacions

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

---

<sup>82</sup> TS 101 456: 7.4.4 d); TS 102 042: 7.4.4 d)

<sup>83</sup> TS 101 456: 7.4.4 e) ; TS 102 042: 7.4.4 e)

<sup>84</sup> TS 101 456: 7.4.4 f) ; TS 102 042: 7.4.4 f)

<sup>85</sup> TS 101 456: 7.4.4 g) ; TS 102 042: 7.4.4 g)

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

### 5.1.2 Accés físic

L'Entitat de Certificació haurà d'establir nivells de seguretat amb restricció d'accés als diferents perímetres i barreres físiques definides.

Per a l'accés a les dependències de l'Entitat de Certificació on es duuguin a terme processos relacionats amb el cicle de vida del certificat, serà necessària l'autorització prèvia, identificació en el moment de l'accés i registre del mateix, incloent filmació per circuit tancat de televisió i el seu arxiu<sup>86</sup>.

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

La generació de claus criptogràfiques de les Entitats de Certificació, així com el seu emmagatzematge, haurà de realitzar-se en dependències específiques per a aquestes finalitats, i requeriran d'accés i permanència dobles.

### 5.1.3 Electricitat i aire condicionat

Els equips informàtics de l'Entitat de Certificació hauran d'estar convenientment protegits davant de fluctuacions o talls de subministrament elèctric, que puguin danyar-los o interrompre el servei.

Les instal·lacions comptaran 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 hauran d'estar ubicats en un entorn on es garanteixi una climatització (temperatura i humitat) adequada a les seves condicions òptimes de treball.

### 5.1.4 Exposició a l'aigua

L'Entitat de Certificació haurà de disposar de sistemes de detecció d'inundacions adequats per protegir els equips i actius davant de tal eventualitat, en el cas que les condicions d'ubicació de les instal·lacions ho fessin necessari.

### 5.1.5 Advertiment i protecció d'incendis

Totes les instal·lacions i actius de l'Entitat de Certificació han de comptar amb sistemes automàtics de detecció i extinció d'incendis.

---

<sup>86</sup> TS 101 456: 7.4.4 a) i d); ; TS 102 042: 7.4.4 a) i d)

En concret, els dispositius criptogràfics i suports que emmagatzemin 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.

### 5.1.6 Emmagatzematge de suports

L'emmagatzematge en suports d'informació ha de realitzar-se de manera que es garanteixi tant la seva integritat com la seva confidencialitat, d'acord amb la classificació de la informació que s'hagi establert<sup>87</sup>.

Haurà de comptar amb dependències o armaris ignífugs.

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

### 5.1.7 Tractament de residus

L'eliminació de suports, tant en paper com magnètics, s'haurà de realitzar mitjançant mecanismes que garanteixin la impossibilitat de recuperació de la informació.

En el cas de suports magnètics, es procedirà al formatat, esborrat permanent o destrucció física del suport.

En el cas de documentació en paper, aquesta haurà de sotmetre's a un tractament físic de destrucció.

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

Periòdicament, l'Entitat de Certificació emmagatzemarà una còpia de seguretat dels sistemes d'informació en dependències físicament separades d'aquelles en les quals es trobin els equips.

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

## 5.2 Controls de procediments

Les Entitats de Certificació han de garantir que els seus sistemes s'operin de forma segura<sup>88</sup>, i per això hauran d'establir i implantar procediments per a les funcions que afectin a la provisió dels seus serveis.<sup>89</sup>

El personal al servei de l'Entitat de Certificació realitzarà els procediments administratius i de gestió d'acord amb la política de seguretat de l'Entitat de Certificació.<sup>90</sup>

---

<sup>87</sup> TS 101 456: 7.4.5 c) i i); TS 102 042: 7.4.5 c) i i)

<sup>88</sup> Art. 20, 1, d) Llei 59/2003; TS 101 456: 7.4.5; TS 102 042: 7.4.5

<sup>89</sup> TS 101 456: 7.4.5 d); TS 102 042: 7.4.5 d)

<sup>90</sup> TS 101 456: 7.4.3 d) ; TS 102 042: 7.4.5 d)

### 5.2.1 Funcions fiables

Les persones que hagin d'ocupar aquests llocs hauran de ser formalment nomenades per l'alta direcció de l'Entitat de Certificació<sup>91</sup>.

Les funcions fiables hauran d'incloure<sup>92</sup>:

- a. Personal responsable de la seguretat
- b. Administradors del sistema
- c. Operadors del sistema
- d. Auditors del sistema
- e. Qualsevol altra persona amb accés a dades de caràcter personal

Les funcions i obligacions fiables hauran de definir-se i documentar-se en la Declaració de Pràctiques de Certificació de l'Entitat de Certificació<sup>93</sup>.

### 5.2.2 Nombre de persones per tasca

Les funcions fiables identificades en la política de seguretat de l'Entitat de Certificació Vinculada i les seves responsabilitats associades seran documentades en descripcions de llocs de treball<sup>94</sup>.

### 5.2.3 Identificació i autenticació per a cada funció

L'Entitat de Certificació haurà d'identificar i autenticar el personal abans d'accedir a la corresponent funció fiable<sup>95</sup>.

### 5.2.4 Rols que requereixen separació de tasques

L'Entitat de Certificació haurà d'identificar, en la seva política de seguretat, funcions o rols fiables.<sup>96</sup>

Les esmentades descripcions hauran de realitzar-se tenint en compte que ha d'existir una separació de funcions sensibles, així com una concessió de mínim privilegi, quan sigui

---

<sup>91</sup> TS 101 456: 7.4.3 h); TS 102 042: 7.4.3 h)

<sup>92</sup> TS 101 456: 7.4.3 g); TS 102 042: 7.4.3 g)

<sup>93</sup> RD 994/99: Art. 9.1

<sup>94</sup> TS 101 456: 7.4.3 b); TS 102 042: 7.4.3 b)

<sup>95</sup> TS 101 456: 7.4.6 e); TS 102 042: 7.4.3 e)

<sup>96</sup> TS 101 456: 7.4.3 b); TS 102 042: 7.4.3 b)



possible. Per determinar la sensibilitat de la funció, es tindran en compte els següents elements<sup>97</sup> :

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

## 5.3 Controls de personal

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

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

Aquest requisit s'aplicarà al personal de gestió de CATCert, especialment en relació amb procediments de personal de seguretat.

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

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

### 5.3.2 Requisits de formació

L'Entitat de Certificació haurà de formar el personal en llocs fiables i de gestió, fins que aconseguixin la qualificació necessària, d'acord amb l'establert a la secció corresponent d'aquesta política.

La formació haurà d'incloure els següents continguts:

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

---

<sup>97</sup> TS 101 456: 7.4.3 c); TS 102 042: 7.4.3 c)

### 5.3.3 Requisits i freqüència d'actualització formativa

Tot el personal vinculat a les ER 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'Entitat de Certificació haurà de disposar d'un sistema sancionador, per depurar les responsabilitats derivades d'accions no autoritzades.

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

### 5.3.6 Requisits de contractació de professionals

L'Entitat de Certificació podrà contractar professionals per a qualsevol funció, fins i tot per a un lloc fiable, cas en el qual s'hauran de sotmetre als mateixos controls que els treballadors restants.

En el cas que el professional no hagi de sotmetre's a aquests controls, haurà d'estar constantment acompanyat per un treballador fiable.

En el cas que tots o una part dels serveis de certificació siguin operats per un tercer, els controls i previsions realitzades en aquesta secció 5, o en altres parts de la política de certificació o de la DPC, seran aplicats i complerts pel tercer que realitzi les funcions d'operació dels serveis de certificació; l'entitat de certificació serà responsable en tot cas de l'efectiva execució.

Aquests aspectes hauran de quedar concretats a l'instrument jurídic utilitzat per acordar la prestació dels serveis de certificació pel tercer diferent de l'entitat de certificació.

### 5.3.7 Subministrament de documentació al personal

L'Entitat de Certificació subministrarà la documentació que estrictament necessiti el seu personal en cada moment, amb la finalitat que sigui prou competent d'acord amb l'establert a la secció corresponent d'aquesta política.

## 5.4 Procediments d'auditoria de seguretat

### 5.4.1 Tipus d'esdeveniments registrats

L'Entitat de Certificació ha de guardar registre, com a mínim, dels següents esdeveniments relacionats amb la seguretat de l'entitat:

- Encès i apagat dels sistemes

- Inici i acabament de l'aplicació d'Autoritat (tècnica) de certificació
- Intents de crear, esborrar, canviar contrasenyes o permisos dels usuaris dins del sistema
- Canvis en les claus de l'Autoritat (tècnica) de certificat
- Canvis en les polítiques d'emissió de certificats
- Intents d'entrada i sortida del sistema
- Intents no autoritzats d'entrada a la xarxa de l'Entitat de Certificació
- Intents no autoritzats d'accés als fitxers del sistema
- Generació de les claus de l'Entitat de Certificació i de les Entitats de Certificació vinculades
- Intents nuls de lectura i escriptura en un certificat i en el directori
- Esdeveniments relacionats amb el cicle de vida del certificat, com una sol·licitud, emissió, revocació i renovació d'un certificat
- Esdeveniments relacionats amb el cicle de vida del mòdul criptogràfic, com a recepció, ús i desinstal·lació d'aquest.

L'Entitat de Certificació també ha de guardar, ja sigui manualment o electrònicament, la següent informació:

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

### 5.4.2 Freqüència de tractament de registres d'auditoria

Els registres d'auditoria s'examinaran almenys una vegada a la setmana a la recerca d'activitat sospitosa o no habitual.

El processament dels registres d'auditoria consisteix en una revisió dels registres que inclou la verificació que aquests no han estat manipulats, una breu inspecció de totes les entrades de registre i una investigació més profunda de qualsevol alerta o irregularitat en

els registres. Les accions realitzades a partir de la revisió d'auditoria també han d'estar 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 corresponent d'aquesta política.

### **5.4.4 Protecció dels registres d'auditoria**

Els fitxers de registre, tant manuals com elèctrics, han de protegir-se de lectures, modificacions, esborrat o qualsevol altre tipus de manipulació no autoritzada usant controls d'accés lògic i físic.

### **5.4.5 Procediments de còpies de seguretat**

S'hauran de generar còpies de seguretat incrementals de registre d'auditoria diàriament i còpies completes setmanalment.

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

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

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

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

Es podrà comunicar 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 hauran de ser guardats, en part, per monitoritzar les vulnerabilitats del sistema.

Les anàlisis de vulnerabilitats han de ser executades, repassades i revisades per mitjà d'un examen d'aquests esdeveniments monitoritzats.

Aquestes anàlisis han de ser executades diàriament, mensualment i anualment d'acord amb la seva definició en el Pla d'Auditoria de l'Entitat de Certificació.

## 5.5 Arxiu d'informacions

L'Entitat de Certificació ha de garantir que tota la informació relativa als certificats es guarda durant un període de temps apropiat<sup>98</sup>, segons l'establert a la secció corresponent d'aquesta política.

### 5.5.1 Tipus d'esdeveniments registrats

L'Entitat de Certificació ha de guardar tots els esdeveniments que tinguin lloc durant el cicle de vida d'un certificat, incloent la renovació d'aquest<sup>99</sup>.

L'Entitat de Certificació ha de guardar un registre del següent:

- Tipus de document presentat a la sol·licitud del certificat
- Número d'identificació únic proporcionat pel document anterior
- Identitat de l'Entitat de Registre que accepta la sol·licitud de certificat<sup>100</sup>
- La ubicació de les còpies de sol·licituds de certificats i de l'acord signat pel subscriptor, en cas de certificats individuals o del posseïdor de les claus en cas de certificats d'organització o d'entitat.<sup>101</sup>

### 5.5.2 Període de conservació de registres

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

L'Entitat de Certificació ha de guardar els registres especificats a la secció corresponent d'aquesta política durant 5 anys, comptats des del moment de l'expedició del certificat.

#### 5.5.2.2 Requisits específics per als certificats reconeguts

L'Entitat de Certificació ha de guardar els registres especificats a la secció corresponent d'aquesta política durant 15 anys, comptats des del moment de l'expedició del certificat.

#### 5.5.2.3 Requisits per als certificats CIC

Per als certificats CIC els registres es guardaran indefinidament.

---

<sup>98</sup> TS 101 456: 7.4.11; TS 102 042: 7.4.11

<sup>99</sup> TS 101 456: 7.4.11 h) ; TS 102 042: 7.4.11 h)

<sup>100</sup> TS 101 456: 7.4.11 i) ; TS 102 042: 7.4.11 i)

<sup>101</sup> TS 101 456: 7.4.11 i) ; TS 102 042: 7.4.11 i)

### 5.5.3 Protecció de l'arxiu

L'Entitat de Certificació ha de:

- Mantenir la integritat i la confidencialitat de l'arxiu que conté les dades referents als certificats emesos.<sup>102</sup>
- Arxivar les dades indicades anteriorment de forma completa i confidencial.<sup>103</sup>
- Mantenir la privacitat de les dades de registre del subscriptor, en cas de certificats individuals, o del posseïdor de les claus, en cas de certificats d'organització o d'entitat.<sup>104</sup>

### 5.5.4 Procediments de còpia de suport

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

L'Entitat de Certificació ha de realitzar còpies de suport incrementals diàries de tots els seus documents electrònics, segons aquesta política. A més, ha de realitzar còpies de suport completes setmanalment per a casos de recuperació de dades, d'acord amb la secció corresponent d'aquesta política.

#### 5.5.4.2 Requisits específics per als certificats personals i d'identitat

L'Entitat de Certificació ha de guardar els documents en paper, segons la secció corresponent, en un lloc fora de les instal·lacions de la mateixa Entitat de Certificació per a casos de recuperació de dades, d'acord amb la secció corresponent d'aquesta política.

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

L'Entitat de Certificació ha d'emetre els certificats i les LRC amb informació de temps i hora. No és necessari que aquesta informació es trobi signada.

### 5.5.6 Localització del sistema d'arxiu

L'Entitat de Certificació ha de tenir un sistema de manteniment de dades d'arxiu fora de les seves pròpies instal·lacions, així com s'especifica a la secció corresponent d'aquesta política.

---

<sup>102</sup> TS 101 456: 7.4.11 a) ; TS 102 042: 7.4.11 a)

<sup>103</sup> TS 101 456: 7.4.11 b) ; TS 102 042: 7.4.11 b)

<sup>104</sup> TS 101 456: 7.4.11 j) ; TS 102 042: 7.4.11 j)

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

Només persones autoritzades per l'Entitat de Certificació podran tenir accés a les dades d'arxiu, sigui a les mateixes instal·lacions de l'Entitat de Certificació o en la seva ubicació externa.

## 5.6 Renovació de claus

Per a la renovació de certificats CIC, l'Entitat de Certificació emissora comprovarà que es continuen complint els requisits que van determinar l'emissió d'aquests certificats.

La sol·licitud del nou certificat serà signada amb la clau privada del certificat CIC a renovar, sempre que aquest es trobi vigent.

Els certificats CIC renovats es comunicaran als usuaris finals, mitjançant la seva publicació en el Registre de CATCert.

## 5.7 Compromís de claus i recuperació de desastre

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

L'Entitat de Certificació establirà en la seva DPC els procediments que aplica en la gestió de les incidències que afectin les seves claus i, molt especialment, en els compromisos de la seguretat de les claus.

### 5.7.2 Corrupció de recursos, aplicacions o dades

Quan tingui lloc un esdeveniment de corrupció de recursos, aplicacions o dades l'Entitat de Certificació ha d'iniciar 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'Entitat de Certificació (o pla de recuperació de desastres) ha de considerar el compromís o sospita de compromís de la clau privada de l'Entitat de Certificació com un desastre.

En cas de compromís l'Entitat de Certificació ha de proporcionar, com a mínim, el següent:

- Informar a tots els subscriptors i verificadors del compromís.
- Indicar que els certificats i la informació de l'estat de revocació lliurats usant la clau d'aquesta Entitat de Certificació ja no són vàlids.<sup>105</sup>

---

<sup>105</sup> TS 101 456: 7.4.8 c); TS 102 042: 7.4.8 c)

## 5.7.4 Desastre sobre les instal·lacions

L'Entitat de Certificació ha de desenvolupar, mantenir, testar i, si és necessari, executar un pla d'emergència en el cas de desastre, ja sigui per causes naturals o causat per l'home, sobre les instal·lacions, que indiqui com restaurar els serveis dels Sistemes d'Informació. La ubicació dels sistemes de recuperació de desastre ha de disposar de les proteccions físiques de seguretat detallades en el Pla de Seguretat.

L'Entitat de Certificació ha de ser capaç de restaurar l'operació normal de la PKI en les 24 hores següents al desastre, podent executar-se, com a mínim, les següents accions:

- Revocació de certificats
- Publicació d'informació de revocació

La base de dades de recuperació de desastres utilitzada per l'Entitat de Certificació ha d'estar 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'Entitat de Certificació han de tenir les mesures de seguretat físiques especificades en el Pla de Seguretat.

## 5.8 Finalització del servei

### 5.8.1 Entitat de Certificació

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

Abans d'acabar els seus serveis, l'Entitat de Certificació ha d'executar, com a mínim, els següents procediments:

- Informar a tots els subscriptors i verificadors (no es requereix que l'Entitat de Certificació tingui alguna relació anterior amb terceres parts).
- Acabar tota autorització de subcontractacions que actuïn en nom de l'Entitat de Certificació en el procés d'emissió de certificats.
- Executar 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.
- Destruir les claus privades de l'Entitat de Certificació o retirar-les de l'ús.

L'Entitat de Certificació ha de declarar en les seves pràctiques les previsions que té per al cas d'acabament del servei. Aquestes han d'incloure:

- Notificació a les entitats afectades
- Transferència de les obligacions de l'Entitat de Certificació a altres persones



- Com es tractarà l'estat de revocació dels certificats emesos que encara no han expirat<sup>106</sup>.

L'Entitat de Certificació podrà transferir els certificats, en els termes previstos en la Llei 59/2003, de 19 de desembre.

## 5.8.2 Entitat de Registre

Sense estipulació addicional.

---

<sup>106</sup> TS 101 456: 7.4.9; TS 102 042: 7.4.9

## 6. Controls de seguretat tècnica

---

L'Entitat de Certificació haurà d'utilitzar sistemes i productes fiables, que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i criptogràfica dels processos de certificació als quals serveixen de suport.<sup>107</sup>

### 6.1 Generació i instal·lació del parell de claus

#### 6.1.1 Generació del parell de claus

##### 6.1.1.1 Requisits per a tots els certificats

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

##### 6.1.1.2 Requisits específics per al CIC

CATCert procedirà a la generació de les claus d'Entitat de Certificació d'acord amb la Cerimònia de Claus, dins del perímetre d'alta seguretat destinat específicament a aquesta tasca.

##### 6.1.1.3 Requisits específics per als certificats de xifratge

Les claus dels certificats de xifratge seran creades per l'Entitat de Registre i, en el seu cas, seran emmagatzemats per a la seva posterior recuperació.

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

Per als certificats de signatura reconeguda i certificats de nivell alt, la clau privada del subscriptor, en certificats individuals, o al posseïdor de claus, en certificats d'organització o d'entitat, li haurà de ser lliurada degudament protegida mitjançant una targeta intel·ligent que compleixi l'establert en un perfil de protecció de dispositiu segur de signatura electrònica d'entitat final normalitzat, d'acord a Common Criteria, EAL 4, o FIPS 140-2 Nivell 3 o superior nivell de seguretat.

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

El mètode de tramesa de la clau pública a l'Entitat de Certificació serà el PKCS #10, una altra prova criptogràfica equivalent o qualsevol altre mètode aprovat per l'Agència Catalana de Certificació.

---

<sup>107</sup> Llei 59/2003: Art. 20.1 d); TS 101 456: 7.4.7; TS 102 042: 7.4.7

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

Les claus d'Entitats de Certificació han de ser comunicades als verificadors, assegurant la integritat de la clau i autenticant l'origen<sup>108</sup>.

La clau pública de CATCert es publicarà en el directori de l'Entitat de Certificació, en forma de certificat autosignat, al costat d'una declaració referent a què la clau permet autenticar a l'Entitat de Certificació.

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

La clau pública de l'Entitat de Certificació Vinculada es publicarà en el directori de l'Entitat de Certificació, en forma de certificat CIC signat per CATCert.

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

### 6.1.5 Mides de les claus

Les claus de les Entitats de Certificació Vinculades seran almenys de 2.048 bits.

Les claus de tots els certificats emesos per les Entitats de Certificació Vinculades 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 realitzarà d'acord amb l'especificació tècnica de l'ETSI TS 001 276, que indica la qualitat dels algorismes de signatura electrònica.

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

Els parells de claus de les Entitats de Certificació (tant de CATCert com de les Entitats de Certificació Vinculades) hauran d'estar generades utilitzant maquinari criptogràfic que compleixi els requisits establerts en un perfil de protecció de dispositiu segur de signatura electrònica d'autoritat de certificació normalitzat, d'acord amb Common Criteria EAL 4, o FIPS 140-2 Nivell 3 o superior nivell de seguretat.

---

<sup>108</sup> TS 101 456: 7.2.3 a); TS 102 042: 7.2.3 a)

Els parells de claus dels subscriptors de certificats de signatura i de certificats de nivell alt, hauran de generar-se en targetes intel·ligents o en dispositius criptogràfics que compleixin els requisits establerts en un perfil de protecció de dispositiu segur de signatura electrònica entitat final normalitzat, d'acord amb Common Criteria EAL 4, o FIPS 140-2 Nivell 3 o superior nivell de seguretat.

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

## 6.1.9 Propòsits d'ús de les claus

L'Entitat de Certificació haurà d'incloure l'extensió *KeyUsage* a tots els certificats, indicant els usos permesos de les corresponents claus privades.

## 6.2 Protecció de la clau privada

### 6.2.1 Mòduls de protecció de la clau privada

#### 6.2.1.1 Estàndards dels mòduls criptogràfics<sup>109</sup>

Les claus privades de les Entitats de Certificació (tant de CATCert com de les Entitats de Certificació Vinculades) hauran de protegir-se utilitzant maquinari criptogràfic que compleixi els requisits establerts en un perfil de protecció de dispositiu segur de signatura electrònica d'autoritat de certificació normalitzat, d'acord amb Common Criteria EAL 4, o FIPS 140-2 Nivell 3 o superior nivell de seguretat.

Els parells de claus dels subscriptors de certificats de signatura i de certificats de nivell alt seran protegits per targetes intel·ligents o en dispositius criptogràfics que compleixin els requisits establerts en un perfil de protecció de dispositiu segur de signatura electrònica d'entitat final normalitzat, d'acord amb Common Criteria EAL 4, o FIPS 140-2 Nivell 3 o superior nivell de seguretat.

La protecció de les claus privades de la resta de certificats podrà realitzar-se mitjançant aplicacions informàtiques.

#### 6.2.1.2 Cicle de vida de les targetes amb circuit integrat

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

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

Quan CATCert detecti errors o defectes en les targetes, podrà retirar d'ofici les targetes afectades. En cas de detectar defectes o errors en casos puntuals, es substituirà la targeta

---

<sup>109</sup> TS 101 456: 7.2.2

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

L'accés a les claus privades de les Entitats de Certificació off-line, haurà de requerir necessàriament del concurs altern de tres (3) dispositius criptogràfics protegits per una clau d'accés, d'entre cinc (5) dispositius. La resta d'Entitats de Certificació Vinculades requerirà del concurs de dos (2) dispositius criptogràfics de cinc (5) possibles.

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

Els dispositius criptogràfics quedaran emmagatzemats a les dependències de l'Entitat de Certificació Vinculades, i per al seu accés serà necessària una persona addicional.

### 6.2.3 Dipòsit de la clau privada

Les claus privades de les Entitats de Certificació s'emmagatzemen en espais ignífugs i protegits per controls d'accés físic doble.

Les claus privades dels certificats personals i d'entitat no es podran emmagatzemar en l'Entitat de Certificació, excepte en cas de certificats de xifratge.

### 6.2.4 Còpia de seguretat de la clau privada

Haurà d'existir còpia de seguretat de la clau privada de l'Entitat de Certificació Vinculada i dels mitjans necessaris per accedir-hi, en una dependència independent d'aquella on s'emmagatzema habitualment.

### 6.2.5 Arxiu de la clau privada<sup>110</sup>

La clau privada de l'Entitat de Certificació haurà de comptar amb una còpia de suport realitzada, emmagatzemada i recuperada, en el seu cas, per personal subjecte a la política de confiança del personal. Aquest personal ha d'estar expressament autoritzat per a aquestes finalitats, i ha de limitar-se a aquell que necessiti fer-ho en les pràctiques de l'Entitat de Certificació.

Haurà de mantenir-se i utilitzar-se protegida per un dispositiu criptogràfic que compleixi els requisits establerts en un perfil de protecció de dispositiu segur de signatura electrònica d'autoritat de certificació normalitzat, d'acord amb Common Criteria EAL 4, o FIPS 140-2 Nivell 3 o superior nivell de seguretat.

---

<sup>110</sup> TS 101 456: 7.2.2

Quan la clau privada de signatura abandoni aquest tipus de dispositius, haurà de fer-ho de forma xifrada.

Els controls de seguretat a aplicar a les còpies de suport de l'Entitat de Certificació hauran de ser d'igual o superior nivell a les que s'apliquin a la claus habitualment en ús.

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

No s'emmagatzemaran còpies de claus privades dels certificats, excepte en casos de certificats de xifrat, en què segons disposi la DPC de l'Entitat de Certificació, aquesta clau privada podrà estar emmagatzemada per garantir la recuperació de dades.

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

Les claus privades de les Entitats de Certificació quedaran emmagatzemades en fitxers xifrats amb claus fragmentades i en targetes intel·ligents (de les quals no podran ser extretes).

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

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

Les claus privades es generaran directament en els mòduls criptogràfics.

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

Per a certificats CIC, es requeriran almenys dues persones per activar la clau privada.

Per a certificats personals i d'entitat, la clau privada del subscriptor s'activarà mitjançant la introducció del PIN a la targeta intel·ligent o de les dades d'activació exigides pel dispositiu criptogràfic.

### **6.2.9 Mètode de desactivació de la clau privada**

Per a certificats personals i d'entitat que incloguin la política bàsica de signatura reconeguda, quan la targeta intel·ligent es retiri del dispositiu lector, o l'aplicació que la utilitzi finalitzi la sessió, serà necessària novament la introducció de les dades d'activació anteriorment indicades.

### **6.2.10 Mètode de destrucció de la clau privada**

Les claus privades seran destruïdes en una forma que impedeixi el seu robatori, modificació, divulgació no autoritzada o ús no autoritzat.

### 6.2.11 Classificació dels mòduls criptogràfics

Els mòduls de les Entitats de Certificació Vinculades s'han de trobar certificats amb el nivell i augments previstos en un perfil de protecció de dispositiu segur de signatura electrònica d'autoritat de certificació normalitzat, d'acord amb Common Criteria EAL 4 o FIPS 140-2 nivell 3.

Els mòduls dels subscriptors de certificats de signatura electrònica reconeguda i de certificats de nivell alt s'han de trobar certificats amb el nivell i augments previstos en un perfil de protecció de dispositiu segur de signatura electrònica d'entitat final normalitzat, d'acord amb Common Criteria EAL 4, o FIPS 140-2 nivell 3.

## 6.3 Altres aspectes de gestió del parell de claus

### 6.3.1 Arxiu de la clau pública

L'Entitat de Certificació arxivarà les seves claus públiques, d'acord amb l'establert a la secció corresponent d'aquesta política.

### 6.3.2 Períodes d'utilització de les claus pública i privada<sup>111</sup>

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

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

## 6.4 Dades d'activació

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

Si l'Entitat de Certificació facilita al subscriptor un dispositiu segur de creació de signatura, llavors les dades d'activació del dispositiu hauran d'estar generades de forma segura per l'Entitat de Certificació.

### 6.4.2 Protecció de dades d'activació

Si l'Entitat de Certificació facilita al subscriptor un dispositiu segur de creació de signatura, les dades d'activació del dispositiu hauran d'estar distribuïdes separatament del mateix dispositiu de creació de signatura (per exemple, lliurant-se en moments diferents, o per rutes diferents).

Com a excepció, quan el subscriptor, en cas de certificats individuals, o el posseïdor de claus, en cas de certificats d'organització o d'entitat, rebí presencialment el seu certificat en

---

<sup>111</sup> TS 101 456: 7.2.6; TS 102 042: 7.2.6

un dispositiu per part d'una Entitat de Registre, podrà seleccionar i introduir les dades d'activació, de manera que les conegui únicament ell.

### 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<sup>112</sup>

S'haurà de garantir que l'accés als sistemes és limitat a individus degudament autoritzats. En particular:

- L'Entitat de Certificació ha de garantir 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'Entitat de Certificació ha de garantir que l'accés als sistemes d'informació i aplicacions es restringeix d'acord a l'establert en la política de control d'accés, així com que els sistemes proporcionen els controls de seguretat suficients per implementar la segregació de funcions identificada en les pràctiques de l'Entitat, incloent la separació de funcions d'administració dels sistemes de seguretat i dels operadors. En concret, l'ús de programes d'utilitats del sistema estarà restringit i estretament controlat.
- El personal de l'Entitat haurà d'estar identificat i reconegut abans d'utilitzar aplicacions crítiques relacionades amb el cicle de vida del certificat.
- El personal de l'Entitat serà responsable i haurà de poder justificar les seves activitats, per exemple mitjançant un arxiu d'esdeveniments.
- Haurà d'evitar-se la possibilitat de revelació de dades sensibles mitjançant la reutilització d'objectes d'emmagatzematge (per exemple fitxers esborrats) que quedin accessibles a usuaris no autoritzats.
- Els sistemes de seguretat i monitoratge han de permetre una ràpida detecció, registre i actuació davant d'intents irregulars d'accés o no autoritzats als seus recursos (per exemple, mitjançant un sistema de detecció d'intrusions, monitoratge i alarma).
- L'accés als dipòsits públics de la informació de l'Entitat (per exemple, certificats o informació d'estat de revocació) haurà de comptar amb un control d'accessos per a modificacions o esborrat de dades.

<sup>112</sup> TS 101 456: 7.4.6; TS 101 456: 7.4.6



## 6.5.2 Avaluació del nivell de seguretat informàtica

Les aplicacions de CA i RA hauran de ser fiables, d'acord amb l'especificació tècnica CEN CWA 14167-1.

## 6.6 Controls tècnics del cicle de vida

### 6.6.1 Controls de desenvolupament de sistemes

S'haurà de realitzar una anàlisi de requisits de seguretat durant les fases de disseny i especificació de requisits de qualsevol component utilitzat en les aplicacions d'Autoritat (tècnica) de certificació i d'Autoritat (tècnica) de Registre, per garantir que els sistemes són segurs<sup>113</sup>.

S'utilitzaran procediments de control de canvis per a les noves versions, actualitzacions i pedaços d'emergència dels esmentats components<sup>114</sup>.

### 6.6.2 Controls de gestió de seguretat

L'Entitat de Certificació haurà de mantenir un inventari de tots els actius informàtics i realitzarà una classificació dels mateixos d'acord amb les seves necessitats de protecció, coherent amb l'anàlisi de riscos efectuada<sup>115</sup>.

La configuració dels sistemes s'auditarà de forma periòdica, d'acord amb l'establert a la secció corresponent d'aquesta política<sup>116</sup>.

Es realitzarà un seguiment de les necessitats de capacitat, i es planificaran procediments per garantir suficient disponibilitat electrònica i d'emmagatzematge per als actius informatius<sup>117</sup>.

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

Sense estipulació addicional.

## 6.7 Controls de seguretat de xarxa<sup>118</sup>

S'haurà de garantir que l'accés a les diferents xarxes de l'Entitat de Certificació és limitat a individus degudament autoritzats. En particular:

---

<sup>113</sup> TS 101 456: 7.4.7 a)

<sup>114</sup> TS 101 456: 7.4.7 b)

<sup>115</sup> TS 101 456: 7.4.2 a)

<sup>116</sup> TS 101 456: 7.4.6 h)

<sup>117</sup> TS 101 456: 7.4.5 f)

<sup>118</sup> TS 101 456: 7.4.6

- Han d'implementar-se controls (com per exemple tallafocs) per protegir la xarxa interna de dominis externs accessibles per terceres parts. Els tallafocs hauran de configurar-se de manera que s'impedeixin accessos i protocols que no siguin necessaris per a l'operació de l'Entitat de Certificació.
- Les dades sensibles hauran de protegir-se quan s'intercanviïn a través de xarxes no segures (incloent les dades de registre del subscriptor).
- S'ha de garantir que els components locals de xarxa (com encaminadors) es trobin 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

Els certificats emesos per l'Agència Catalana de Certificació i les Entitats de Certificació adscrites a la jerarquia pública de certificació de Catalunya tindran el contingut i els camps descrits al document "perfil de certificat" corresponent, que l'Agència Catalana de Certificació ha de publicar en el seu directori.

En tot cas, el perfil de cada certificat inclourà en la seva estructura, com a mínim, les següents dades:

- a. Número de sèrie, que serà un codi únic respecte al nom distingit de l'emissor.
- b. Algorisme de signatura, amb algun dels algorismes identificats a la secció corresponent d'aquesta política.
- c. El nom distingit de l'emissor, d'acord amb la secció corresponent d'aquesta política.
- d. Inici de validesa del certificat, en Temps Coordinat Universal, codificat d'acord amb la RFC 2459.
- e. Final de validesa del certificat, en Temps Coordinat Universal, codificat d'acord amb la RFC 2459.
- f. Nom distingit del subjecte, d'acord amb la secció corresponent d'aquesta política.
- g. Clau pública del subjecte, codificada d'acord amb RFC 2459
- h. Signatura, generada i codificada d'acord amb RFC 2459

Tots els certificats seran conformes amb les següents normes:

1. RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, January 1999
2. ITU-TU Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997

Adicionalment, els certificats reconeguts seran conformes amb les següents normes:

1. ETSI TS 101 862 v1.2.1 (2001-06): Qualified Certificate Profile, 2001
2. RFC 3039: Internet X.509 Public Key Infrastructure - Qualified Certificate Profile, 2001 (sempre que no entri en conflicte amb TS 101 862)

Així mateix, els certificats reconeguts hauran de contenir els següents camps<sup>119</sup>:

- a. La indicació que s'expedeixen com a certificats reconeguts
- b. El codi identificatiu únic del certificat

---

<sup>119</sup> Llei 59/2003: Art. 11.2

- c. La identificació del prestador de serveis de certificació que expedeix el certificat, indicant el nom o raó social, domicili, adreça electrònica i número d'identificació fiscal.
- d. La signatura electrònica avançada del prestador de serveis de certificació que expedeix el certificat.
- e. La identificació del signant (el subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització o d'entitat), pel seu nom i cognoms i DNI o equivalent, o a través d'un pseudònim que consti de manera inequívoca.
- f. En els supòsits de representació, la indicació del document que acrediti les facultats del signant per actuar en nom de la persona física o jurídica que representa.
- g. Les dades de verificació de signatura que corresponguin a les dades de creació de signatura que es trobin sota el control del signant.
- h. El començament i el final del període de validesa del certificat.
- i. Els límits d'ús del certificat, si es preveuen.
- j. Els límits del valor de les transaccions per a les quals pot utilitzar-se el certificat, si s'estableixen.

### 7.1.1 Número de versió

Tots els certificats contindran un camp amb el número de versió, indicant que es tracta de certificats de versió 3.

### 7.1.2 Extensions de certificat

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

### 7.1.3 Identificadors d'objecte d'algoritmes

L'Entitat de Certificació podrà utilitzar el següent algoritme de signatura:

sha-1WithRSAEncryption OID = {iso (1) member-body (2) us (840) rsadsi (1.13549) pkcs (1) pkcs-1 (1) 5}

### 7.1.4 Formats de noms

L'Entitat de Certificació emplenarà els camps de noms dels certificats amb les informacions establertes en el perfil corresponent de certificat, publicat en el web de CATCert (<http://www.catcert.cat/>).

### 7.1.5 Restriccions de noms

Sense estipulació addicional.

### 7.1.6 Identificador d'objecte de política de certificat

L'Entitat de Certificació emplenarà l'extensió política de certificat amb els identificadors d'objecte establerts a la secció corresponent d'aquesta política, quan s'adhereixin directament a ella mateixa.

En cas de crear la seva pròpia política, en els casos permesos per aquesta política de certificats, inclourà l'identificador d'objecte específicament definit a l'efecte.

### 7.1.7 Ús de l'extensió restriccions de política

Sense estipulació addicional.

### 7.1.8 Sintaxi i semàntica dels qualificadors de política<sup>120</sup>

L'Entitat de Certificació inclourà als certificats un qualificador de política, amb els següents elements:

- CPS Pointer
- explícit Text

CPS Pointer haurà d'incloure una referència URI a les condicions generals de verificació dels certificats emesos per l'Entitat de Certificació.

explícit Text haurà de contenir una declaració concisa relativa al certificat<sup>121</sup>.

### 7.1.9 Semàntica del procés de l'extensió crítica de política de certificat

Sense estipulació addicional

### 7.1.10 Especificacions tècniques per a totes les Entitats de Certificació

Les Entitats de Certificació han de respectar els usos tecnològics generalment acceptats i s'han d'adaptar a les bones pràctiques i als requeriments tècnics més avançats.

---

<sup>120</sup> RFC 2459: 4.2.1.5

<sup>121</sup> Vegi's secció corresponent 5

Adicionalment, la renovació de les Entitats de Certificació immediatament posterior a la present versió de la Política General haurà de respectar les següents especificacions tècniques:

- L'algoritme utilitzat ha de ser objecte de renovació quan existeixi un risc de descriptació advertit per la comunitat. Les Entitats de Certificació incorporaran, posteriorment a la emissió d'aquesta Política General, l'algoritme SHA-256.
- Els números de sèrie dels certificats hauran de ser sempre en enters i, en tot cas, positius.
- S'utilitzarà la codificació UTF-8.
- Es simplificarà l'extensió "authorityKeyIdentifier".
- Es restringiran els *OIDs* generats per les entitats de certificació intermèdies.

## 7.2 Perfil de la llista de revocació de certificats

### 7.2.1 Número de versió

Sense estipulació addicional.

### 7.2.2 Llista de revocació de certificats i extensions d'elements de la llista

Les llistes de revocació de certificats emeses per l'Agència Catalana de Certificació i les Entitats de Certificació adscrites a la jerarquia pública de certificació de Catalunya tindran el contingut i camps descrits al document "perfil de llista de revocació de certificats" corresponent, que l'Agència Catalana de Certificació publica en el seu web (<http://www.catcert.cat/>).

## 8. Auditoria de conformitat

L'Entitat de Certificació Vinculada ha de realitzar periòdicament una auditoria de conformitat per provar que compleix, una vegada ha començat a funcionar, els requisits de seguretat i d'operació necessaris per formar part de la jerarquia pública de certificació de Catalunya.

A més de l'auditoria de conformitat, l'Entitat de Certificació Vinculada ha d'estar preparada per passar altres revisions, no periòdiques, que demostrin la seva confiança:

- Abans d'acceptar una nova Entitat de Certificació subordinada a la jerarquia, l'Agència Catalana de Certificació ha de realitzar una revisió dels seus documents de seguretat, DPC i PdC per assegurar que compleix els requisits de seguretat i d'operació necessaris per formar part de la Jerarquia d'Entitats de Certificació de l'Agència Catalana de Certificació.
- Si se sospita que, en qualsevol moment, una vegada l'Entitat de Certificació Vinculada ha començat a funcionar, l'Entitat de Certificació Vinculada no compleix algun dels requisits de seguretat o si s'ha detectat un compromís de claus, ja sigui una sospita o compromís real, o qualsevol esdeveniment que pugui suposar un perill per a la seguretat o integritat de l'Entitat de Certificació Vinculada, es durà a terme una auditoria interna.

L'Entitat de Certificació Vinculada pot delegar l'execució de les auditories a una tercera entitat que, en aquest cas, ha de cooperar completament amb el personal que porti a terme la investigació.

### 8.1 Freqüència de l'auditoria de conformitat

L'Entitat de Certificació Vinculada ha de portar a terme una auditoria de conformitat anualment, a més de les auditories internes que pugui portar a terme 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

Si l'Entitat de Certificació Vinculada disposa d'un departament d'auditoria interna, aquest podrà encarregar-se de portar a terme l'auditoria de conformitat.

En el cas de no tenir aquest departament, l'Entitat de Certificació Vinculada podrà 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 han d'estar portades a terme per una entitat independent de l'Entitat de Certificació Vinculada auditada. En cas de auditoria

interna, l'auditor no ha de tenir cap conflicte d'interessos que afecti negativament la seva capacitat de portar a terme serveis d'auditoria.

## 8.4 Relació d'elements objecte d'auditoria

Els elements objecte d'auditoria seran els següents:

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

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

Una vegada s'obté l'informe de l'auditoria de compliment portada a terme, l'Entitat de Certificació Vinculada ha de discutir, amb l'entitat que ha executat l'auditoria i amb CATCert, les deficiències trobades i desenvolupa i executa un pla correctiu que solucioni les esmentades deficiències.

Si l'Entitat de Certificació Vinculada auditada és incapaç de desenvolupar i/o executar l'esmentat pla o si les deficiències trobades suposen una amenaça immediata per a la seguretat o integritat del sistema haurà de realitzar-se una de les següents accions:

- Revocar la clau de l'Entitat de Certificació Vinculada, de la forma com es descriu a les seccions corresponents d'aquesta política.
- Acabar el servei de l'Entitat de Certificació Vinculada, de la forma com es descriu a la secció corresponent d'aquesta política.

## 8.6 Tractament dels informes d'auditoria

L'Entitat de Certificació Vinculada ha de lliurar 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 establirà les tarifes que aplicaran totes les Entitats de Certificació Vinculades, a la prestació dels seus serveis.

Aquestes tarifes poden trobar-se al web de CATCert (<http://www.catcert.cat/tarifes/>).

CATCert no practicarà reintegraments. En cas de productes defectuosos, es procedirà a substituir el producte defectuós per un altre en bon estat.

#### 9.1.2 Tarifa d'accés a certificats

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

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

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

#### 9.1.4 Tarifes d'altres serveis

Sense estipulació addicional.

#### 9.1.5 Política de reintegració

Sense estipulació addicional.

### 9.2 Capacitat financera

#### 9.2.1 Assegurança de responsabilitat civil

L'Entitat de Certificació haurà de disposar 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, excepte quan es trobi eximida per Llei d'aquesta obligació. Aquesta assegurança cobreix les actuacions de CATCert com a prestador de serveis de certificació.

En cas d'ús incorrecte o no autoritzat dels certificats, CATCert (o l'EC corresponent) no actuarà com agent fiduciari front a subscriptors i terceres 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'assegurança per a subscriptors i tercers que confiïn en certificats

Sense estipulació addicional.

## 9.3 Confidencialitat

### 9.3.1 Informacions confidencials

Les següents informacions seran mantingudes com a confidencials per l'Entitat de Certificació:

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

### 9.3.2 Informacions no confidencials

Les següents informacions no tindran caràcter confidencial:

- a. Les Declaracions de Pràctiques de Certificació de totes les Entitats de Certificació
- b. Tota altra informació identificada com a "Pública"

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

L'Entitat de Certificació Vinculada serà responsable de l'establiment de les mesures apropiades de protecció de la informació confidencial.

Aquestes mesures inclouran les apropiades clàusules 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 9.4
- b. Mesures, normes, procediments, regles i estàndards que garanteixin el nivell de seguretat exigida pel RD 1720/2007 - secció 9.4, i, en general, tots els controls tècnics de les seccions 5 i 6 de la Política General de Certificació de CATCert.
- c. Funcions i obligacions del personal (article 89 del RD 1720/2007) - secció 5.3.
- d. Registre d'incidències (article 90 del RD 1720/2007), procediment de notificació, gestió i resposta davant les incidències – secció 9.4.5
- e. Control d'accés (article 91 del RD 1720/2007) – seccions 5 i 6.
- f. Gestió de suports (article 92 del RD 1720/2007) – secció 5.
- g. Identificació i autenticació (article 93 del RD 1720/2007) – secció 5.2.
- h. Procediments de còpia de seguretat i recuperació de dades (article 94 del RD 1720/2007) - secció 5.5.5.5

### 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'Entitat de Certificació Vinculada serà l'única entitat que gaudirà dels drets de propietat intel·lectual sobre els certificats que emeti.

L'Entitat de Certificació Vinculada haurà de concedir llicència no exclusiva per reproduir, distribuir, verificar i utilitzar els certificats, sense cap cost, en relació amb signatures digitals i/o sistemes de xifrat dins de l'àmbit d'aplicació d'aquesta política, d'acord amb el corresponent instrument vinculant entre l'Entitat de Certificació Vinculada i la part que reproduceix i/o distribueix el certificat.

Les anteriors normes figuraran als instruments jurídics que existeixin entre l'Entitat de Certificació Vinculada i els subscriptors i els verificadors.

Addicionalment, els certificats emesos per l'Entitat de Certificació Vinculada han de contenir un avís legal relatiu a la propietat d'aquests.

Aquesta normativa resultarà d'aplicació en l'ús d'informació de revocació de certificats.



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

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

Cada Entitat de Certificació Vinculada serà propietària de la seva Declaració de Pràctiques de Certificació.

## 9.5.3 Propietat de la informació relativa a noms

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

El subscriptor o, en el seu cas, el posseïdor de claus serà el propietari del nom distingit del certificat, format per les informacions especificades a la secció corresponent d'aquesta política.

## 9.5.4 Propietat de claus

Els parells de claus seran propietat dels subscriptors dels certificats.

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

## 9.6 Obligacions i responsabilitat civil

### 9.6.1 Entitats de Certificació

#### 9.6.1.1 Obligacions i altres compromisos

##### ***Obligacions de CATCert***

CATCert té les següents obligacions:

- Operar l'Entitat de Certificació Arrel de manera diligent, d'acord amb les polítiques, pràctiques i normativa de la jerarquia pública de certificació de Catalunya.
- Operar les seves Entitats de Certificació Vinculades, pròpies o que donin serveis a les Entitats de Certificació Virtuals, d'acord amb allò disposat per l'apartat 9.6.1.1.2.
- 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 aquestes compleixin les obligacions previstes per l'apartat 9.6.1.1.2.

##### ***Obligacions de les Entitats de Certificació Vinculades***

Les Entitats de Certificació Vinculades s'obligaran a complir el següent:



- a. L'Entitat de Certificació Vinculada ha de garantir sota la seva plena responsabilitat, que compleix amb tots els requisits establerts en aquesta política de certificació<sup>122</sup>.
- b. L'Entitat de Certificació Vinculada serà l'única entitat responsable del compliment dels procediments descrits en aquesta política, inclòs quan una part o la totalitat de les operacions siguin subcontractades externament<sup>123</sup>.
- c. L'Entitat de Certificació Vinculada ha de prestar els seus serveis de certificació d'acord amb la seva Declaració de Pràctiques de Certificació vigent<sup>124</sup>, en la que es detallaran almenys els continguts previstos a l'article 19 de la Llei 59/2003.
- d. Abans de l'emissió i lliurament del certificat al subscriptor, l'Entitat de Certificació Vinculada haurà d'informar-lo dels aspectes previstos a l'article 18.b) de la Llei 59/2003<sup>125</sup>, i dels següents aspectes:
  - a) Indicació de la política aplicable, amb indicació de si els certificats s'expedeixen al públic i de la necessitat d'utilització de dispositiu segur de creació de signatura<sup>126</sup>.
  - b) Forma en la qual es garanteix la responsabilitat patrimonial de l'Entitat de Certificació<sup>127</sup>.
  - c) Si l'Entitat de Certificació ha estat declarada conforme amb la política de certificació i, en el seu cas, d'acord amb quin sistema. En concret, la certificació del prestador de serveis de certificació<sup>128</sup> i la certificació dels productes de signatura electrònica utilitzats<sup>129</sup>.
- e. Aquest requisit es complirà mitjançant un "Text divulgatiu de la política de certificat" aplicable, que podrà ser transmesa electrònicament, utilitzant un mitjà de comunicació durador en el temps, i en llenguatge comprensible<sup>130</sup>.
- f. L'Entitat de Certificació Vinculada ha d'obligar els subscriptors, als posseïdors de claus i als verificadors mitjançant instruments jurídics apropiats a cada situació.
- g. Aquests instruments jurídics podran ser transmesos electrònicament, hauran d'estar en llenguatge escrit i comprensible, i han de tenir els següents continguts mínims<sup>131</sup>:
  - a) Prescripcions per donar compliment a l'establert en la present política de certificació.

<sup>122</sup> TS 101456: 6.1 primer; TS 102042: 6.1 primer

<sup>123</sup> TS 101456: 6.1 segon; TS 102042: 6.1 segon

<sup>124</sup> TS 101456: 6.1 quart; TS 102042: 6.1 tercer

<sup>125</sup> TS 101456: 7.3.1 a) i b); TS 102042: 7.3.1 a) i c)

<sup>126</sup> TS 101456: 7.3.4

<sup>127</sup> Llei 59/2003: Art. 26

<sup>128</sup> Llei 59/2003: Art. 26

<sup>129</sup> Llei 59/2003: Art. 27

<sup>130</sup> TS 101456: 7.3.1 a) i b); TS 102042: 7.3.1 a) i c)

<sup>131</sup> TS 101456: 7.3.4; TS 102 042: 7.3.4

- b) 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.
  - c) Manifestació que la informació continguda al certificat és correcta, excepte notificació en contra pel subscriptor<sup>132</sup>.
  - d) Consentiment per a la publicació del certificat en el directori i accés per tercers al mateix<sup>133</sup>.
  - e) 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 a tercers, en cas d'acabament d'operacions de l'Entitat de Certificació Vinculada<sup>134</sup> sense revocació de certificats vàlids.
  - f) Límits d'ús del certificat, incloent els establerts a la secció 4.5 d'aquesta política.
  - g) 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 al certificat, que resulta aplicable quan el subscriptor actua com a verificador.
  - h) Limitacions de responsabilitat aplicables, incloent els usos pels quals l'Entitat de Certificació Vinculada accepta o exclou la seva responsabilitat.
  - i) Procediments aplicables de resolució de disputes.
  - j) Llei aplicable i jurisdicció competent.
- h. L'Entitat de Certificació Vinculada ha d'identificar el subscriptor del certificat, d'acord amb els articles 12 i 13 de la Llei 59/2003 i la present política de certificat i, en concret:
- a) L'Entitat de Certificació Vinculada ha de comprovar per si mateixa o per mitjà d'una Entitat de Registre, la identitat i qualssevol altres circumstàncies personals dels sol·licitants dels certificats, d'acord amb l'establert a l'article 13 de la Llei 59/2003.
  - b) En cas que el subscriptor del certificat de persona física (certificat de classe 1 o certificat de classe 2 de col·lectiu) sigui una persona jurídica, l'Entitat de Certificació Vinculada ha de comprovar que el posseïdor de la clau es troba degudament autoritzat pel subscriptor.
- i. L'Entitat de Certificació Vinculada ha de complir la resta d'obligacions contingudes a l'article 12 de la Llei 59/2003.

### Requisits específics per als certificats personals i d'entitat

<sup>132</sup> TS 101456: 7.3.1 h) cinquè; TS 102 042: 7.3.1 l) cinquè

<sup>133</sup> TS 101456: 7.3.1 h) quart; TS 102042: 7.3.1 l) quart

<sup>134</sup> TS 101456: 7.3.1 h) tercer; TS 102042: 7.3.1 l) tercer

L'Entitat de Certificació ha d'assumir altres obligacions incorporades directament al certificat o incorporades per referència<sup>135</sup>.

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

Adicionalment a l'establert a la secció corresponent, l'instrument jurídic que vincula l'Entitat de Certificació Vinculada i el subscriptor haurà d'estar en llenguatge escrit i comprensible, i ha de tenir els següents continguts mínims:

- a. Indicació de la política aplicable, amb indicació de si els certificats s'expedeixen al públic o a una comunitat tancada d'usuaris i de la necessitat d'ús de dispositiu segur de creació de signatura<sup>136</sup>.
- b. Certificació de serveis de l'Entitat de Certificació Vinculada<sup>137</sup>.
- c. Forma en la qual es garanteix la responsabilitat patrimonial de l'Entitat de Certificació Vinculada<sup>138</sup>.

#### **Requisits específics per al CDS, CDSCD i CDS-1 de Seu electrònica**

L'Entitat de Certificació ha de comprovar el nom de domini, i altres dades tècniques, com l'IP, que hagin de figurar al certificat.

### ***Obligacions de l'Entitat de Certificació Virtual***

Les Entitats de Certificació Virtual s'obligaran a complir el següent:

- a. Determinar la comunitat de subscriptors i verificadors de l'Entitat de Certificació Vinculada.
- b. Aprovar les polítiques de certificació i, si és necessari, les polítiques específiques de certificació.
- c. Aprovar, si és necessari, la Declaració de Pràctiques de Certificació.
- d. Aprovar la documentació contractual i reguladora dels serveis de certificació en la comunitat d'usuaris de l'Entitat de Certificació Vinculada.
- e. Notificar puntualment l'Entitat de Certificació Vinculada de totes les informacions relatives als canvis a realitzar, incidències en el servei, reclamacions, denúncies i inspeccions del servei.

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

---

<sup>135</sup> TS 101 456: 6.1 tercer

<sup>136</sup> TS 101 456: 7.3.4

<sup>137</sup> Llei 59/2003: Art. 26

<sup>138</sup> Llei 59/2003: Art. 20.2

### 9.6.1.2 Garanties ofertes a subscriptors i a verificadors

L'Entitat de Certificació Vinculada, com a mínim, garantirà al subscriptor:

- a. El compliment de les seves obligacions legals com a prestador de serveis de certificació, d'acord amb la Llei 59/2003, de 19 de desembre.
- b. Que no hi hagi errors de fet en les informacions contingudes als certificats, coneguts o realitzats per l'Entitat de Certificació Vinculada i, en el seu cas, per l'Entitat de Registre.
- c. Que no hi hagi errors de fet en les informacions contingudes als certificats, deguts a falta de diligència en la gestió de la sol·licitud de certificat o a la creació d'aquest.
- d. Que els certificats compleixin tots els requisits materials establerts en la DPC.
- e. Que els serveis de revocació i l'ús del directori compleixin tots els requisits materials establerts en la DPC.

L'Entitat de Certificació Vinculada, com a mínim, garantirà al verificador:

- a. El compliment de les seves obligacions legals com a prestador de serveis de certificació, d'acord amb la Llei 59/2003, de 19 de desembre.
- b. Que la informació continguda o incorporada per referència al certificat és correcta, excepte quan s'indiqui el contrari.
- c. En cas de certificats publicats en el directori, que el certificat ha estat emès al subscriptor identificat en aquest i que el certificat ha estat acceptat, d'acord amb la secció corresponent de la present política de certificació.
- d. Que en l'aprovació de la sol·licitud de certificat i en l'emissió del certificat s'han complert tots els requisits materials establerts en la DPC.
- e. La rapidesa i seguretat en la prestació dels serveis, en especial dels serveis de revocació.

Adicionalment, l'Entitat de Certificació garantirà al subscriptor i al verificador:

- a. Que el certificat conté les informacions que ha de contenir un certificat reconegut, d'acord amb l'article 11.2 de la Llei 59/2003, de 19 de desembre.
- b. Que, en el cas que generi les claus privades del subscriptor o, en el seu cas, el posseïdor de claus, es manté la seva confidencialitat durant el procés<sup>139</sup>.
- c. La responsabilitat de l'Entitat de Certificació, amb els límits que s'estableixin.

---

<sup>139</sup> Llei 59/2003: Art. 20.1.e)

## 9.6.2 Entitats de Registre

### 9.6.2.1 Obligacions i altres compromisos

#### ***Obligacions de les Entitats de Registre Internes***

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

- a. Actuar exclusivament en relació amb persones vinculades a l'Entitat de Registre Interna.
- b. Nomenar com a operadors de l'autoritat (tècnica) de registre, a dos o a més dels seus treballadors (depenent de l'EC, generalment, quatre o més), i comunicar a CATCert les dades corresponents a aquestes persones per a l'emissió dels certificats d'operador corresponents. Quan un operador deixi de tenir capacitat per actuar com el que és, sota el control i l'autoritat de l'Entitat de Registre Interna, aquesta Entitat de Registre Interna ha de sol·licitar de forma immediata a l'Entitat de Certificació Vinculada la revocació del certificat d'operador corresponent.
- c. Validar i aprovar les sol·licituds de certificats i generar els certificats per als posseïdors de claus, d'acord amb els procediments i instruments tècnics establerts per l'Entitat de Certificació Vinculada, d'acord amb la DPC i la documentació d'operacions de l'Entitat de Certificació Vinculada.
- d. Si l'Entitat de Registre Interna no disposés d'informació actualitzada del posseïdor de claus, comprovar la identitat personalment o d'acord amb l'establert a l'article 13.4 de la Llei 59/2003, i registrar un justificant acreditatiu del nom complet, lloc i data de naixement, DNI i/o qualsevol altra informació que pogués ser utilitzada per diferenciar una persona respecte una altra en l'àmbit de l'Entitat de Registre Interna.
- e. Verificar, quan sigui necessari, qualsevol atribut específic del posseïdor de claus, i registrar un justificant acreditatiu de la informació.
- f. Realitzar o tramitar les sol·licituds de suspensió, habilitació, revocació i renovació de certificats, d'acord amb els procediments i els instruments tècnics establerts per a l'Entitat de Certificació Vinculada, d'acord amb la Declaració de Pràctiques de Certificació, i la documentació d'operacions de l'Entitat de Certificació Vinculada.
- g. Emmagatzemar els registres, ja sigui en paper, ja sigui de forma electrònica, amb les adequades mesures de seguretat, autenticitat, integritat i conservació, relatius a la informació continguda al certificat, durant un període de 15 anys. Aquests registres han d'estar a disposició de l'Entitat de Certificació Vinculada.

#### ***Entitat de Registre Virtual***

L'Entitat de Registre Virtual s'obligarà a complir el següent:

- a. Aportar la justificació documental necessària per al registre d'usuaris i per a la posterior emissió de certificats per part de l'Entitat de Certificació Vinculada o l'Entitat de Registre Col·laboradora.
- b. La justificació documental haurà de ser realitzada per una unitat orgànica de l'Entitat de Registre Virtual facultada legalment per donar fe de les dades a certificar, que s'indicarà a CATCert.

### **Entitat de Registre Col·laboradora**

L'Entitat de Certificació podrà delegar algunes funcions a Entitats de Registre Col·laboradores<sup>140</sup>, que en aquest cas quedaran obligades al seu compliment, en les mateixes condicions que l'Entitat de Certificació.

L'Entitat de Registre Col·laboradora assistirà als subscriptors de certificats de classe 1 amb Entitat de Registre Virtual, i a tots els subscriptors de certificats de classe 2.

L'Entitat de Registre Col·laboradora actuarà en el seu propi nom, sense perjudici de la responsabilitat de l'Entitat de Certificació Vinculada.

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

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

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

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

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

#### **9.6.2.2 Garanties ofertes a subscriptor i verificadors**

##### **Garantia de CATCert pels serveis de certificació digital**

CATCert garanteix que la clau privada de l'entitat de certificació utilitzada per emetre certificats no ha estat compromesa, a excepció de que CATCert hagués comunicat el contrari mitjançant el registre de certificació de CATCert, de conformitat amb la Declaració de pràctiques de certificació.

CATCert únicament garanteix que:

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

---

<sup>140</sup> Art 13.5. Llei 59/2003

- b) No ha originat ni ha introduït declaracions falses o errònies en la informació de cap certificat, ni ha deixat d'incloure informació necessària aportada pel subscriptor i validada per CATCert o per l'entitat de registre col·laboradora, en el moment de l'emissió del certificat.
- c) Tots els certificats compleixen els requisits formals i de contingut de la seva Declaració de pràctiques de certificació.
- d) Queda vinculada pels procediments operatius, de seguretat i d'arxiu descrits en la Declaració de pràctiques de certificació.

### ***Exclusió de la garantia***

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

## **9.6.3 Subscriptors**

### **9.6.3.1 Obligacions i altres compromisos**

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

L'Entitat de Certificació Vinculada obligarà<sup>141</sup> al subscriptor a:

- a. Facilitar a l'Entitat de Certificació Vinculada informació completa i adequada, conforme als requeriments d'aquesta política de certificació, en especial pel que respecta al procediment de registre<sup>142</sup>.
- 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 la present política de certificació 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 corresponent.
- e. Notificar a l'Entitat de Certificació Vinculada, sense endarreriments injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu segur de creació de signatura.
- f. Notificar a l'Entitat de Certificació Vinculada i qualsevol persona que el subscriptor cregui que pugui confiar en el certificat, sense endarreriments injustificables<sup>143</sup>:
  - a) La pèrdua, el robatori o el compromís potencial de la seva clau privada.

---

<sup>141</sup> No s'estableix cap requisit sobre la manera en la qual s'hauria de complir aquest requisit: podrà ser mitjançant contracte o mitjançant un altre instrument jurídic.

<sup>142</sup> TS 101 456: 6.2.a) es considera una obligació que ha de ser genèrica per a tots els tipus de certificats sol·licitats per subscriptors.

<sup>143</sup> TS 101 456: 6.2.g)



- b) La pèrdua de control sobre la seva clau privada, a causa del compromís de les dades d'activació (per exemple, el codi PIN del dispositiu segur de creació de signatura) o per qualsevol altra causa.
- c) Les inexactituds o canvis en el contingut del certificat que conegui o pugués conèixer el subscriptor.
- g. Deixar d'utilitzar la clau privada transcorregut el període indicat a la secció corresponent.
- h. Transferir als posseïdors de claus les obligacions específiques d'aquests.
- i. No monitorar, manipular o realitzar actes d'enginyeria inversa sobre la implantació tècnica de la jerarquia, sense permís previ per escrit.
- j. No comprometre intencionadament la seguretat de la jerarquia pública de certificació de Catalunya.

### ***Requisits específics per als certificats de signatura electrònica reconeguda***

L'Entitat de Certificació Vinculada obligarà el subscriptor a:

- a. Utilitzar el parell de claus exclusivament per a signatures electròniques i conforme a qualsevol altra limitació que li sigui notificada<sup>144</sup>.
- b. Reconèixer que aquestes signatures electròniques són signatures electròniques equivalents a signatures manuscrites, d'acord amb l'article 3.4 de la Llei 59/2003, de 19 de desembre.
- c. Ser especialment diligent en la custòdia de la seva clau privada i del seu dispositiu segur de creació de signatura, a fi d'evitar usos no autoritzats<sup>145</sup>.
- d. Si el subscriptor genera les seves pròpies claus, s'obliga a:
  - 1. Generar les seves claus de subscriptor utilitzant un algorisme reconegut com a acceptable per a la signatura electrònica reconeguda<sup>146</sup>.
  - 2. Crear la claus dins del dispositiu segur de creació de signatura<sup>147</sup>.
  - 3. Utilitzar longituds i algorismes de clau reconeguts com a acceptables per a la signatura electrònica reconeguda<sup>148</sup>.
- e. Notificar a l'EC, sense endarreriments injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu segur de creació de signatura.

---

<sup>144</sup> TS 101 456: 6.2.b)

<sup>145</sup> TS 101 456: 6.2.c), més estricte, i extensió al dispositiu segur de creació de signatura.

<sup>146</sup> TS 101 456: 6.2.d) primer

<sup>147</sup> TS 101 456: 6.2.f)

<sup>148</sup> TS 101 456: 6.2.d) segon



### 9.6.3.2 Garanties ofertes pel subscriptor

L'Entitat de Certificació Vinculada haurà d'obligar el subscriptor, mitjançant el corresponent instrument jurídic, a garantir:

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

### 9.6.3.3 Protecció de la clau privada

L'Entitat de Certificació Vinculada haurà d'obligar el subscriptor, mitjançant el corresponent instrument jurídic, a garantir que el subscriptor és l'únic responsable dels danys causats pel seu incompliment de l'haver de protegir la clau privada.

## 9.6.4 Verificadors

### 9.6.4.1 Obligacions i altres compromisos

L'Entitat de Certificació Vinculada ha d'obligar l'usuari de certificats<sup>149</sup> 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<sup>150</sup>.
- c. Verificar tots els certificats de la jerarquia de certificats, abans de confiar en la signatura digital o en algun dels certificats de la jerarquia.
- d. Tenir present qualsevol limitació en l'ús del certificat, amb independència que es trobi al mateix certificat o al contracte de verificador<sup>151</sup>.

---

<sup>149</sup> Típicament, mitjançant unes condicions generals d'ús del certificat.

<sup>150</sup> TS 101 456: 6.3 a); TS 102 042: 6.3 a)

<sup>151</sup> TS 101 456: 6.3 b); TS 102 042: 6.3 b)

- e. Tenir present qualsevol precaució establerta en un contracte o en un altre instrument, amb independència de la seva naturalesa jurídica<sup>152</sup>.
- f. No monitorar, manipular o realitzar actes d'enginyeria inversa sobre la implantació tècnica de la jerarquia pública de certificació de Catalunya, sense permís previ per escrit.
- g. No comprometre intencionadament la seguretat de la jerarquia pública de certificació de Catalunya.
- h. Reconèixer que les signatures electròniques produïdes per certificats reconeguts de signatura reconeguda són signatures electròniques equivalents a signatures escrites, d'acord amb l'article 3.4 de la Llei 59/2003, de 19 de desembre.

#### 9.6.4.2 Garanties ofertes pel verificador

L'Entitat de Certificació haurà d'obligar al verificador, mitjançant el corresponent instrument jurídic, a manifestar:

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

#### 9.6.5 Altres Participants

##### 9.6.5.1 Obligacions i garanties del directori

L'Entitat de Certificació Vinculada podrà delegar algunes funcions en el directori, que en aquest cas estarà obligat al seu compliment, en les mateixes condicions que l'Entitat de Certificació.

Les funcions, obligacions i deures del directori s'establiran detalladament en la Declaració de Pràctiques de Certificació de l'Entitat de Certificació Vinculada, així com en la documentació jurídica auxiliar, especialment la lliurada a subscriptors, posseïdors de claus i verificadors.

##### 9.6.5.2 Garanties ofertes pel directori

L'Entitat de Certificació Vinculada ha d'establir en la seva DPC la responsabilitat civil del directori quan sigui operat per una tercera entitat.

---

<sup>152</sup> TS 101 456: 6.3 c); TS 102 042: 6.3 c)

## 9.7 Renúncies de garanties

### 9.7.1 Rebuig de garanties de l'Entitat de Certificació

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

## 9.8 Limitacions de responsabilitat

### 9.8.1 Limitacions de responsabilitat de l'Entitat de Certificació vinculada

L'Entitat de Certificació Vinculada limitarà 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 l'Entitat de Certificació.

L'Entitat de Certificació Vinculada podrà limitar la seva responsabilitat mitjançant la inclusió de límits d'ús del certificat<sup>153</sup>, i límits de valor de les transaccions per a les quals es pot utilitzar el certificat<sup>154</sup>.

### 9.8.2 Cas fortuït i força major

L'Entitat de Certificació Vinculada inclourà 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.

---

<sup>153</sup> Llei 59/2003: 11.2.h)

<sup>154</sup> Llei 59/2003: 11.2.i)

## 9.10 Termini i acabament

### 9.10.1 Termini

L'Entitat de Certificació Vinculada haurà d'establir, als seus instruments jurídics amb els subscriptors i els verificadors, una clàusula que determini el període de vigència de la relació jurídica en virtut de la qual subministra certificats als subscriptors.

### 9.10.2 Acabament

L'Entitat de Certificació Vinculada haurà d'establir, als seus instruments jurídics amb els subscriptors i els verificadors, una clàusula que determini les conseqüències de l'acabament de la relació jurídica en virtut de la que subministra certificats als subscriptors.

### 9.10.3 Supervivència

L'Entitat de Certificació Vinculada haurà d'establir, als seus instruments jurídics amb els subscriptors i els verificadors, clàusules de supervivència, en virtut de les quals certes regles continuessin vigents després de l'acabament de la relació jurídica reguladora del servei entre les parts.

A aquest efecte, l'Entitat de Certificació Vinculada vetllarà perquè, almenys els requisits continguts a les seccions Obligacions, Responsabilitat civil, Auditoria de conformitat i Confidencialitat, continuïn vigents després de l'acabament de la política de certificació i dels instruments jurídics que vinculin l'Entitat de Certificació amb subscriptors i verificadors.

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

## 9.11 Notificacions

L'Entitat de Certificació Vinculada haurà d'establir, als seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules de notificació.

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

## 9.12 Modificacions

### 9.12.1 Procediment per a les modificacions

Les Entitats de Certificació Vinculades podran modificar, de forma unilateral, la política de certificació, sempre que procedeixin segons el següent procediment:

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

### 9.12.2 Període i mecanismes per a notificacions

Les modificacions de la política es notificaran a CATCert, per a la seva posterior aprovació.

### 9.12.3 Circumstàncies en què un OLD ha de ser canviat

Sense estipulació addicional.

## 9.13 Resolució de conflictes

### 9.13.1 Resolució extrajudicial de conflictes

L'Entitat de Certificació Vinculada haurà d'establir, als seus instruments jurídics amb subscriptors i verificadors, els procediments de mediació i resolució de conflictes aplicables<sup>155</sup>.

Amb aquesta finalitat, es tindrà en compte la consideració com a Administració Pública de l'Entitat de Certificació Vinculada.

Les situacions de discrepància que es derivin de l'ús dels certificats emesos per l'Entitat de Certificació Vinculada, es resoldran aplicant els mateixos criteris de competència que en els casos dels documents signats per escrit.

---

<sup>155</sup> TS 101 456: 7.5.1 h); TS 102042: 7.5.1 h)

### 9.13.2 Jurisdicció competent

L'Entitat de Certificació Vinculada haurà d'establir, als seus instruments jurídics vinculants amb subscriptors i verificadors, una clàusula de jurisdicció competent, indicant que la competència judicial internacional correspon als jutges espanyols.

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

Quan l'Entitat de Certificació Vinculada tingui la consideració d'Administració Pública es tindrà en compte la legislació administrativa que resulti aplicable.

### 9.14 Llei aplicable

L'Entitat de Certificació Vinculada haurà d'establir, 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'Entitat de Certificació Vinculada estigui establerta en l'Estat Espanyol, i/o els seus serveis de certificació es prestin per mitjà d'un establiment permanent situat en l'Estat Espanyol<sup>156</sup>.
- Per a les Entitats de Certificació Vinculades a la jerarquia amb la consideració d'Administració Pública, la normativa administrativa corresponent, estatal i autonòmica.

### 9.15 Conformitat amb la llei aplicable

L'Entitat de Certificació Vinculada haurà de manifestar el compliment de la Llei 59/2003, de 19 de desembre, de signatura electrònica i de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic, en la seva Declaració de Pràctiques de Certificació i amb els instruments jurídics amb subscriptors i verificadors.

### 9.16 Clàusules diverses

#### 9.16.1 Acord íntegre

L'Entitat de Certificació haurà d'establir, als seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules d'acord íntegre.

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

---

<sup>156</sup> Llei 59/2003: 1.2

### 9.16.2 Subrogació

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

En cas que es produeixi una cessió o subrogació, es procedirà a l'acabament de l'Entitat de Certificació Vinculada.

Els drets i els deures associats a la condició d'Entitat de Certificació Virtual podran ser objecte, en canvi, de cessió i subrogació, però aquestes incidències hauran de ser notificades a CATCert.

### 9.16.3 Divisibilitat

L'Entitat de Certificació haurà d'establir, els seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules de divisibilitat.

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

Per al cas que, com a causa als articles 7 i 8 de la Llei 7/1998 sobre condicions generals de la contractació, es consideressin no incorporades al contracte, o nul·les algunes o qualsevol de les clàusules indicades, la no incorporació referida o nul·litat no determinarà la ineficàcia total del contracte, si aquest pogués subsistir sense les clàusules indicades<sup>157</sup>.

### 9.16.4 Aplicacions

Sense estipulació addicional.

### 9.16.5 Altres clàusules

Sense estipulació addicional.

---

<sup>157</sup> Llei 7/1998: Art. 10

**ANNEX I****Control documental**

Projecte:	<b>Informe modificació del document PGdC</b>
Entitat de destí:	<b>Agència Catalana de Certificació</b>
Codi de referència:	<b>Revisió 2n semestre 2011</b>
Versió:	<b>Canvis de la v3.5 a la 3.6 en català i en castellà</b>
Data de l'edició:	<b>03/11/2011</b>

**Control de versions PGdC 2n semestre 2011**

<b>Versió</b>	<b>Parts que canvien</b>	<b>Descripció del canvi</b>	<b>Autor del canvi</b>	<b>Data del canvi</b>
3.5	Apartat 7.1.10	Afegit nou apartat	Oficina de Polítiques	Novembre 2011